

16. 9. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

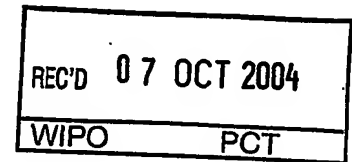
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 3 0 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 4 0 0 7 6
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 3 4 0 0 7 6]

出 願 人 ソニー株式会社
Applicant(s):

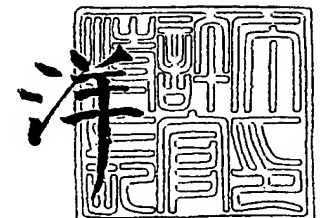


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 7 月 2 6 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 0390389920
【提出日】 平成15年 9月30日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G11B 7/00
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
 【氏名】 木谷 聡
【特許出願人】
 【識別番号】 000002185
 【氏名又は名称】 ソニー株式会社
【代理人】
 【識別番号】 100082762
 【弁理士】
 【氏名又は名称】 杉浦 正知
 【電話番号】 03-3980-0339
【選任した代理人】
 【識別番号】 100120640
 【弁理士】
 【氏名又は名称】 森 幸一
【手数料の表示】
 【予納台帳番号】 043812
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0201252

【書類名】特許請求の範囲**【請求項 1】**

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第 1 の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号手段と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

上記第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記暗号化されて記録されている第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化手段と、

暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

第 1 の暗号化鍵を保持する保持手段と、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号手段と、

上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号手段と、

上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化手段と、

上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号手段と、

上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化手段と、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

【請求項 2】

請求項 1 において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

【請求項 3】

請求項 1 において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

【請求項 4】

請求項 1 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

【請求項5】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

生成された第2の暗号化鍵で上記第3の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記暗号化された第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化手段と、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

第1の暗号化鍵を保持する保持手段と、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復号手段と、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号手段と、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復号化手段と、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復号手段と、

上記記録再生装置に対して伝送するコンテンツ情報を上記第3の暗号化で暗号化する暗号化手段と、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

【請求項6】

請求項5において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

【請求項7】

請求項5において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

【請求項8】

請求項5において、

さらに、暗号化された上記第3の暗号化鍵に対する第1のマスク制御手段と、暗号化された上記第2の暗号化鍵に対する第2のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵および暗号化された上記第2の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

【請求項9】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第1の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

【請求項10】

請求項9において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

【請求項11】

請求項9において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

【請求項12】

請求項9において、

さらに、暗号化された上記第3の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

【請求項13】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を上記第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

上記第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

【請求項14】

請求項13において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

【請求項15】

請求項13において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

【請求項16】

請求項13において、

さらに、暗号化された上記第3の暗号化鍵に対する第1のマスク制御手段と、暗号化された上記第2の暗号化鍵に対する第2のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵および暗号化された上記第2の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

【請求項17】

伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第1の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化手段と、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記暗号化およびバス暗号化されたコンテンツ情報は、上記第3の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

【請求項18】

請求項17において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

【請求項19】

請求項17において、

さらに、暗号化された上記第3の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

【請求項20】

伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

生成された第2の暗号化鍵で上記第3の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、上記暗号化された第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化手段と、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記暗号化およびバス暗号化されたコンテンツ情報は、上記第3の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

【請求項21】

請求項20において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

【請求項22】

請求項20において、

さらに、暗号化された上記第3の暗号化鍵に対する第1のマスク制御手段と、暗号化された上記第2の暗号化鍵に対する第2のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵および暗号化された上記第2の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

【請求項 23】

伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第1の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

【請求項 24】

請求項 23 において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

【請求項 25】

請求項 23 において、

さらに、暗号化された上記第3の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

【請求項 26】

伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を上記第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

上記第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、
上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

【請求項 27】

請求項 26 において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

【請求項 28】

請求項 26 において、

さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御手段と、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

【請求項 29】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

上記記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

上記第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化ステップと、

暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

第 1 の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号ステップと、

上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

【請求項 30】

請求項 29 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

【請求項 31】

請求項 29 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

【請求項 32】

請求項 29 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御ステップを有し、上記認証ステップによって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

【請求項 33】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

上記記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵で上記第 3 の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化ステップと、

暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

第 1 の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号ステップと、

上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

【請求項 34】

請求項 33 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

【請求項 35】

請求項 33 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

【請求項 36】

請求項 33 において、

さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御ステップと、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御ステップとを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

【請求項 37】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

上記記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

【請求項 38】

請求項 37 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

【請求項 39】

請求項 37 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱

数に著作権関連情報を混合するようにした記録方法。

【請求項 40】

請求項 37 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御ステップを有し、
上記認証ステップによって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

【請求項 41】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

上記記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵を上記第 1 の暗号化鍵で暗号化する暗号化ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

上記第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

【請求項 42】

請求項 41 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

【請求項 43】

請求項 41 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

【請求項 44】

請求項 41 において、

さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御ステップと、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御ステップとを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

【請求項 45】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第

1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第1の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復号ステップと、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第3の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

【請求項46】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

生成された第2の暗号化鍵で上記第3の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報

報処理装置に伝送する第2のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第1の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復号ステップと、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第3の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

【請求項47】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

【請求項48】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、
第1の暗号化鍵を保持する保持ステップと、
第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、
生成された第2の暗号化鍵を上記第1の暗号化鍵で暗号化する暗号化ステップと、
第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、
上記第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化ステップと、
情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化ステップと、
上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

【請求項49】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第1の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復号ステップと、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第3の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

【請求項50】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

生成された第2の暗号化鍵で上記第3の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第1の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復号ステップと、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第3の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

【請求項51】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

【請求項52】

記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第1の暗号化鍵を保持する保持ステップと、

第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

生成された第2の暗号化鍵を上記第1の暗号化鍵で暗号化する暗号化ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

上記第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

【書類名】明細書

【発明の名称】信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体

【技術分野】

【0001】

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディア例えばDVD (Digital Versatile Disc)規格のディスクにコンテンツを記録し、また、ディスクメディアからコンテンツを再生する場合に適用される信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体に関する。

【背景技術】

【0002】

近年開発されたDVD等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように、大量の映像情報等をデジタル情報として記録することが可能になると、不正コピーを防止して著作権者の保護を図ることが益々重要になってくる。

【0003】

例えば、DVD-Videoでは、CSS (Content Scramble System)と呼ばれる著作権保護技術が採用されている。DVDに関する著作権保護の方法に関しては、下記の非特許文献1および非特許文献2説明されている。

【0004】

【非特許文献1】「2部知的財産権保護 ソフトウェア復号のカギを握る不正コピー防止技術にメド」, 日経エレクトロニクス 1997.8.18, p.110-119

【非特許文献2】山田, 「DVDを起点に著作権保護空間を広げる」, 日経エレクトロニクス 2001.8.13, p.143-153

【0005】

図1は、これらの文献に説明されているCSS方式の概要を示す。この方式の場合には、3つの暗号化鍵データが使用される。3つの暗号化鍵データは、CSS鍵発行センターが発行するマスターキーと、著作権者等が決めるディスクキーおよびタイトルキーである。マスターキーは、秘密とされ、メーカー毎に異なる固定の値の鍵であり、ディスクキーは、ディスク毎に異なる値の鍵である。何れのマスターキーでも復号できるようなディスクキーのセットが作成され、そのセットがディスクに格納される。ディスクキーをディスクに格納する場合に暗号化されており、セキュアドディスクキーと呼ばれる。

【0006】

ビデオデータ、オーディオデータなどのコンテンツデータを圧縮したMP EG (Moving Picture coding Experts Group)データ1に対して、そのコンテンツに割当てられた暗号化鍵であるタイトルキー2を用意する。さらに、1枚毎のディスクに割当てられた暗号化鍵であるディスクキー3を用意する。そして、暗号化の管理を行う鍵発行センター4では、そのセンター4が管理するマスターキー5を使用して、ディスクキー3を暗号化回路（以下、適宜エンクリプタと称する）6によって暗号化し、さらにディスクキー3を使用してタイトルキー2をエンクリプタ7によって暗号化する。そして、MP EGデータ1に対してタイトルキー2によってスクランブラ8で暗号化する。

【0007】

暗号化されたコンテンツデータ（以下、スクランブルドMP EGデータまたはスクランブルドコンテンツと適宜称する）9と、暗号化されたディスクキー（以下、セキュアドディスクキーと適宜称する）10と、暗号化されたタイトルキー（以下、暗号化タイトルキーと適宜称する）11とがDVD-Videoディスク製造時にDVD-Videoディスク12に記録される。セキュアドディスクキーがディスク12のリードインエリアの所定の位置に記録され、暗号化タイトルキーがセクタ構造化されたコンテンツデータの各セクタに記録される。これらのセキュアドディスクキーおよび暗号化タイトルキーは、著作権保護システム用の鍵情報であり、両者をまとめてCSSキーと称する。

【0008】

図2に示すように、DVDプレイヤーによってDVD-Videoディスク12が再生され、スクランブルDMP EGデータ9、セキュアドディスクキー10および暗号化タイトルキー11が再生され、DVDプレイヤー21に読み込まれる。DVDプレイヤー21では、マスターキー22を使用して暗号化の復号回路（以下、適宜デクリプタと称する）23によってディスクキーを復号し、復号したディスクキーを使用してデクリプタ24によってタイトルキーを復号し、復号したタイトルキーを使用してデスクランブラ25によってMP EGデータを復号する。MP EGデコーダ26によってオーディオ／ビジュアルデータ27が復号される。

【0009】

図3は、ディスク再生時にプレイヤーが最初に読み取り出す領域であるリードインエリアのデータ構成を示す。リードインエリアは、物理的なセクタ番号が0h（hは16進数表記であることを示す記号：以下同じ）から30000hのセクタまで使用され、最初に全ての値が0のエリアが配置され、その後に参照用コードが配置され、再度全ての値が0のエリアが配置され、その後にコントロールデータエリアが設けられている。その後、さらに全ての値が0のエリアがあり、セクタ番号30000hからコンテンツデータが記録されるメインデータエリアとなる。

【0010】

コントロールデータエリアは、最初の1セクタ（セクタ0）に物理フォーマット情報が配置され、次の1セクタ（セクタ1）にディスク製造情報が配置され、次の14セクタ（セクタ2～15）にコンテンツ供給者の情報が配置される。このセクタ0からセクタ15までの16セクタの情報が、コントロールデータエリアに繰り返し配置される。そして、コンテンツ・プロバイダー・インフォメーション（コンテンツ供給者の情報）が配置される区間に、そのディスクに特有のセキュアドディスクキーが配置される。

【0011】

また、タイトルキーが記録される構造について、図4に示すセクタ構造例に基づいて説明すると、コンテンツデータなどのメインデータが記録されるそれぞれのセクタは、2064バイトで構成される。この2064バイトの内の先頭の4バイトがセクタ番号などを示すIDデータとされ、続いた2バイトがIDデータエラー検出用データとされる。さらに次の6バイトがコピー管理用データとされ、このコピー管理用データの中に暗号化タイトルキーが配置される。そして、コピー管理用データに続いた2048（2K）バイトがコンテンツデータなどが記録されるメインデータの記録エリアとされる。さらに、最後の4バイトには、このセクタ全体のエラー検出用データが配置される。

【0012】

このようにディスクキーとタイトルキーを使用して暗号化されてデータが格納されるディスクは、基本的に再生専用のディスクであるが、DVD規格の中には、記録が可能な規格のディスクも存在する。例えば、DVD-RW／-R規格のディスク、DVD+RW／+R規格のディスクは、データの記録が可能であり、いわゆるビットバイビットコピー（bit by bit copy）と称される他の媒体から再生したデジタルデータを、そのまま別の媒体に記録させる処理を行って、DVD-Videoから読出したデータを、これらの規格のディスクにそのまま記録させることで、DVD-Videoディスクのビデオデータなどのコンテンツデータのコピーを不正に作成することができる。しかしながら、上述したディスクキーとタイトルキーが用意されることで、不正にコピーされたビデオデータなどのコンテンツデータが復号できないようになされる。

【0013】

この不正にコピーされたディスクでは、暗号化からの正しい復号ができない点について、図5を参照して説明する。まず、セキュアドディスクキーと暗号化タイトルキーとが上述した配置で記録されたDVD-VideoのディスクDaを用意して、そのディスクDaをユーザが再生する。プレイヤー内では、そのディスクの最内周部のリードインエリアからセキュアドディスクキーが得られ、コンテンツデータが記録されたセクタからは、暗号化

タイトルキーが得られる。セキュアドディスクキーがマスターキーによって復号され、暗号化タイトルキーがディスクキーによって復号される。タイトルキーによって、スクランブルドMPEGデータが復号され、オーディオ／ビジュアルデータが得られる。

【0014】

このDVD-VideoのディスクDaに記録されたコンテンツデータをDVD-RW/R規格のディスクDbに、ビットバイビットコピーで記録させることをユーザが実行したとする。ここで、ディスクDbは、リードインエリアの一部がディスク製造時にビットで書込み済みのエリアとしてあり、その書込み済みのエリアに、そのディスクDbに割当てられたディスクキー又は無効なキーが予め書き込んである。

【0015】

したがって、ディスクDbのデータ記録可能エリアに、DVD-VideoのディスクDaから読出したコンテンツデータをそのまま記録させたDVD-R/RW規格のディスクDb'をユーザが制作した場合、ディスクDb'は、元のディスクDaとはディスクキーが異なっている。ディスクキーが元のディスクDaとは異なるために、コピーされたディスクDb'をユーザが再生しようとしても、プレイヤーでは、正しく復号することができず、結果的に不正コピーが防止されることになる。

【0016】

なお、ここでは主としてDVD-Videoのディスクに適用されるCSS方式の場合について説明したが、DVDオーディオのディスクなどに適用されるスクランブル方式であるCPM(Content Protection for Pre-Recorded)方式の場合にも、基本的な原理は同じである。

【0017】

図6は、CSS方式で記録されたROMディスク例えばDVD-Videoディスクを再生するPCとドライブでのディスクキーとタイトルキーの取り出し方、およびスクランブルデータのデスクランブルの方法を示すものである。図6において、参照符号31がCSSで記録されたDVD-Videoディスクを再生する再生装置としてのDVDドライブを示す。参照符号51がデータ処理装置としてのPCを示す。PC41に対してDVDプレイヤーアプリケーションソフトウェアがインストールされる。

【0018】

DVDドライブ31とPC41との間が標準的なインターフェースで接続されている。インターフェースは、ATAPI(AT Attachment with Packet Interface), SCSI(Small Computer System Interface), USB(Universal Serial Bus), IEEE(Institute of Electrical and Electronics Engineers)1394等である。

【0019】

DVDドライブ31には、認証部32、バスエンクリプタ33および34が備えられている。PC41には、認証部42、バスエンクリプタ43および44が備えられている。認証部32および認証部42は、相互認証を行い、認証動作の度に異なるセッションキー(バスキーとも呼ばれる)Ksを生成する。また、PC41には、マスターキー45、デクリプタ46および47、デスクランブラ48が備えられ、デスクランブラ48から得られたMPEGデータがMPEGデコーダ49で復号されることによってオーディオ／ビジュアルデータ50が得られる。

【0020】

なお、認証動作は、電源のON後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【0021】

DVD-Videoディスクから得られたスクランブルドMPEGデータ9、セキュアドディスクキーが10、暗号化タイトルキー11がDVDドライブ31に読み込まれる。コンテンツデータが記録されたセクタからは、暗号化タイトルキーが得られる。セキュアドデ

ディスクキーがマスターキーによって復号され、暗号化タイトルキーがディスクキーによって復号される。タイトルキーによって、スクランブルDMPEGデータが復号され、オーディオ/ビジュアルデータが得られる。

【0022】

図7は、図6に示す現行のシステムにおいて、DVDドライブ31とPC41との間の信号の授受の手順を示す。PC41がDVDドライブ31に対してコマンドを送り、DVDドライブ31がコマンドに応答した動作を行う。DVD-Videoディスクの挿入等でシーケンスが開始し、最初に認証シーケンスAKE (Authentication and Key Exchange) (ステップS1) がなされる。相互認証が成立すると、セッションキーKsをDVDドライブ31とPC41が共有する。認証が成立しなかった場合では、処理が中断する。

【0023】

次に、PC41からの要求に応じてDVD-Videoディスク12上のコンテンツデータゾーンがシークされ、読み出される(ステップS2)。次のステップS3において、セキュアドディスクキーをPC41がドライブ31に対して要求し、ドライブ31がDVD-Videoディスク12からセキュアドディスクキーを読み取る(ステップS4, S5)。セキュアドディスクキーがセッションキーKsを使用してバスエンクリプタ33によって暗号化される。Ksで暗号化されたセキュアドディスクキーがドライブ31からPC41に戻される(ステップS6)。

【0024】

次に、暗号化タイトルキーおよびコピー世代管理情報CGMS (Copy Generation Management System) をPC41がドライブ31に対して要求し(ステップS7)、ドライブ31がDVD-Videoディスク12から暗号化タイトルキーおよびCGMSを読み取る(ステップS8, S9)。暗号化タイトルキーおよびCGMSがセッションキーKsを使用してバスエンクリプタ34によって暗号化される。Ksで暗号化された暗号化タイトルキーおよびCGMSがドライブ31からPC41に戻される(ステップS10)。

【0025】

次に、スクランブルドコンテンツ(スクランブルDMPEGデータと同一の意味である)をPC41がドライブ31に対して要求し(ステップS11)、ドライブ31がDVD-Videoディスク12からスクランブルドコンテンツを読み取る(ステップS12, S13)。スクランブルドコンテンツがドライブ31からPC41に戻される(ステップS14)。

【0026】

上述したCSS方式は、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSS方式の利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのまるごとコピー(ビットバイビットコピー)することは、CSS契約上では、認められた行為ではない。

【0027】

しかしながら、CSSの暗号方式が破られる事態が発生した。CSSの暗号化を解除してDVD-Videoの内容を簡単にハードディスクにコピーすることを可能とする「DeCSS」と呼ばれるソフトウェアがインターネット上で配布された。「DeCSS」が出現した背景には、本来耐タンパー化が義務付けられているはずのCSS復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にCSSアルゴリズム全体が解読された経緯がある。

【0028】

CSSの後に、DVD-Audio等のDVD-ROMの著作権保護技術であるCPPM (Content Protection for Pre-Recorded Media)、並びに記録型DVD、メモリカードに関する著作権保護技術CPRM (Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、シ

システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。すなわち、CPRMは、ビットバイビットコピーを禁止するため、リードインエリアの鍵情報を記録するエリアを予め記録済みとしている。CPRMは、ライセンス管理者である米4C Entity, LLCが配布する下記の資料（非特許文献3）に説明されている。

【0029】

【非特許文献3】 "Content Protection for Recordable Media Specification DVD Book"、インターネット<URL: <http://www.4Centity.com/>>

【発明の開示】**【発明が解決しようとする課題】****【0030】**

しかしながら、市場に既に大量に供給されたDVDプレイヤーは、後から規格化されたCPRMへ対応しておらず、また、CPRM規格化後のDVDプレイヤーもコスト的な理由からCPRMへ対応しないものが殆どである。したがって、既存のDVD-Videoプレイヤーとの互換性を考慮すると、CPRMを採用しにくい。一方、BSデジタル放送および地上波デジタル放送の実用化と共に、放送コンテンツの著作権の保護のために、放送の暗号化記録に対する必要性が増大している。

【0031】

「DeCSS」が出現してきた状況において、コンテンツの著作権を保護する他の方法として、予めオーディオ/ビジュアルデータに電子透かし情報を埋め込んでおくことが考えられる。電子透かし情報は、コピー後でも保存されるので、再生時に電子透かし情報を検出して再生を禁止することが可能である。

【0032】

しかしながら、電子透かし情報を埋め込む方法は、いくつかの問題があり、実際に行うことが難しい。すなわち、オーディオ/ビジュアル情報の単位より小さい単位でのランダムアクセスが可能なこと、ATAPIという一つのチャンネルを介して読み出しデータと書き込みデータが流れること、電子透かし情報の検出のための回路規模が大きく、コスト負担が重いこと、電子透かし情報の検出のための処理時間が長くなるために、ドライブ本来の書き込み時間や読み出し時間の短縮化の妨げとなること等が存在する。

【0033】

電子透かし情報を使用しないで、DVD-Videoの違法なコピーを防止するために、ドライブが読み出しデータフィルタおよび書き込みデータフィルタを備えるものが提案されている。読み出しデータフィルタは、ディスクから読み出したデータがDVD-Videoデータのビデオ、オーディオ、サブピクチャの何れかの種類のパックであれば、当該パックに対してマスク処理を行い、それ以外の制御情報のパックであれば、マスク処理を行わずに、パックをバッファメモリへ転送する。マスク処理とは、対象のデータを無効データ例えば全てゼロのデータに置き換える処理を意味する。このようにしてDVD-Videoコンテンツの違法な再生を防止できる。

【0034】

書き込みデータフィルタは、PCから転送されてきたパックのパックヘッダを検出してパックの種類を判定し、データがDVD-Videoデータのビデオ、オーディオ、サブピクチャの何れかの種類のパックであれば、当該パックに対してマスク処理を行い、それ以外の制御情報のパックであれば、マスク処理を行わずに、パックをDVDエンコーダへ転送する。したがって、PCによってDVD-Videoのコンテンツが違法にコピーされることを防止することができる。

【0035】

この方法は、PCと書き込み可能なDVDディスクとを利用した違法な再生および記録をDVD-Videoのフォーマットに基づいて防止することができる。しかしながら、DVD-Videoのフォーマットのデータの記録再生が一切できなくなる問題がある。この点を考慮して、PCとドライブとの間で認証を行い、認証が成立しない時には、上述したようなDVDドライブでコンテンツデータのマスク処理を行うモードとし、認証が成立した時

には、コンテンツデータの暗号化／復号を行うモードとする方法が提案されている。この方法は、DVD-Videoディスクを再生することを可能とする。しかしながら、先に提案されている方法では、書き込み時には、コンテンツデータに対してスクランブルをかけていない。

【0036】

書き込みデータに対してスクランブルをかけていないために、既存のDVD-VideoのプレイヤーのCSSを利用することができず、また、記録されたコンテンツデータが著作権が保護されたコンテンツとならない問題があった。たとえCSSの暗号化を破る「DecCSS」ソフトウェアが存在している状況下でも、記録されているコンテンツが正規のライセンス機関の承認を受けたCSSでもってスクランブルがかけられていることは、著作権が保護されるコンテンツであることを明示する上で重要である。

【0037】

よって、この発明の目的は、ドライブによって書き込み時に著作権保護技術例えばCSSによって、書き込みデータを保護し、書き込まれたデータが保護の対象であることを明示することが可能な信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体を提供することにある。

【0038】

また、この発明は、著作権保護技術を一般ユーザの所有するPCのアプリケーションとして搭載する場合に、一般ユーザによる著作権保護技術の書き込みソフトウェアを作成させないようにできる信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体を提供することにある。

【課題を解決するための手段】

【0039】

上述した課題を解決するために、この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第1の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、暗号化されて記録されている第2の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第1のバス暗号化手段と、

暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第2のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

第1の暗号化鍵を保持する保持手段と、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、バス暗号化された第2の暗号化鍵をセッションキーによってバス復号して暗号化された第2の暗号化鍵を復号する第1のバス復号手段と、

暗号化された第2の暗号化鍵を第1の暗号化鍵で復号する復号手段と、
バス暗号化された第3の暗号化鍵をセッションキーによってバス復号して暗号化された第3の暗号化鍵を復号する第2のバス復号化手段と、
暗号化された第3の暗号化鍵を第2の暗号化鍵で復号する復号手段と、
記録再生装置に対して伝送するコンテンツ情報を第3の暗号化で暗号化する暗号化手段と、
暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

【0040】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

生成された第2の暗号化鍵で第3の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、暗号化された第2の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第1のバス暗号化手段と、

暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第2のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

第1の暗号化鍵を保持する保持手段と、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

、バス暗号化された第2の暗号化鍵をセッションキーによってバス復号して暗号化された第2の暗号化鍵を復号する第1のバス復号手段と、

暗号化された第2の暗号化鍵を第1の暗号化鍵で復号する復号手段と、

バス暗号化された第3の暗号化鍵をセッションキーによってバス復号して暗号化された第3の暗号化鍵を復号する第2のバス復号化手段と、

暗号化された第3の暗号化鍵を第2の暗号化鍵で復号する復号手段と、

記録再生装置に対して伝送するコンテンツ情報を第3の暗号化で暗号化する暗号化手段と、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

【0041】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、
第1の暗号化鍵を保持する保持手段と、
記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、
第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、
第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、
情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、
情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、
コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化手段と、
暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、
情報処理装置は、
記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、
記録再生装置に対して伝送するコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

【0042】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、
記録再生装置は、
第1の暗号化鍵を保持する保持手段と、
第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、
生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、
第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、
第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化手段と、
情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、
情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、
コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化手段と、
暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、
情報処理装置は、
記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、
コンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

【0043】

この発明は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、
第1の暗号化鍵を保持する保持手段と、
記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、
第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、
情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

暗号化されて記録されている第2の暗号化鍵をセッションキーによってバス暗号化して
情報処理装置に伝送する第1のバス暗号化手段と、

暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に
伝送する第2のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス
復号手段と、

暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記
録手段とを有し、

暗号化およびバス暗号化されたコンテンツ情報は、第3の暗号化鍵で暗号化され、さら
に、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化した
ものである記録再生装置である。

【0044】

この発明は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し
、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵
と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用し
たコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再
生装置であって、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

生成された第2の暗号化鍵で第3の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

暗号化された第2の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に
伝送する第1のバス暗号化手段と、

暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に
伝送する第2のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス
復号手段と、

暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテ
ンツ情報を記録媒体に記録する記録手段とを有し、

暗号化およびバス暗号化されたコンテンツ情報は、第3の暗号化鍵で暗号化され、さら
に、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化した
ものである記録再生装置である。

【0045】

この発明は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し
、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵
と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用し
たコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再
生装置であって、

第1の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第1の暗号化鍵で復
号する第2の暗号化鍵復号手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化手段と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置である。

【0046】

この発明は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化手段と、暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置である。

【0047】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

暗号化されて記録されている第2の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第2のバス暗号化ステップと、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

第1の暗号化鍵を保持する保持ステップと、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

バス暗号化された第2の暗号化鍵をセッションキーによってバス復号して暗号化された第2の暗号化鍵を復号する第1のバス復号ステップと、

暗号化された第2の暗号化鍵を第1の暗号化鍵で復号する復号ステップと、

バス暗号化された第3の暗号化鍵をセッションキーによってバス復号して暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

暗号化された第3の暗号化鍵を第2の暗号化鍵で復号する復号ステップと、

記録再生装置に対して伝送するコンテンツ情報を第3の暗号化で暗号化する暗号化ステップと、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

【0048】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第1の暗号化鍵を保持する保持ステップと、

第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

生成された第2の暗号化鍵で第3の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

暗号化された第2の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第2のバス暗号化ステップと、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

第1の暗号化鍵を保持する保持ステップと、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

バス暗号化された第2の暗号化鍵をセッションキーによってバス復号して暗号化された第2の暗号化鍵を復号する第1のバス復号ステップと、

暗号化された第2の暗号化鍵を第1の暗号化鍵で復号する復号ステップと、

バス暗号化された第3の暗号化鍵をセッションキーによってバス復号して暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

暗号化された第3の暗号化鍵を第2の暗号化鍵で復号する復号ステップと、

記録再生装置に対して伝送するコンテンツ情報を第3の暗号化で暗号化する暗号化ステップと、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

【0049】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化ステップと、

暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

記録再生装置に対して伝送するコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

【0050】

この発明は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第1の暗号化鍵を保持する保持ステップと、

第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化ステップと、

暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

【発明の効果】**【0051】**

この発明では、暗号化例えばCSS方式でコンテンツ情報を記録するので、記録されたコンテンツ情報は、著作権が保護されたものであることを明確とできる。すなわち、正規のライセンスを受けない違法な方法で、記録されているコンテンツ情報をコピーしたり、再生すれば、著作権を侵害していると主張することができる。この発明では、記録再生装置内で生成した暗号化鍵を記録再生装置自身がメディア例えばDVDディスクへ書き込むことにより、CSS方式でDVDディスクへ記録をするときに、一般のPCユーザがCSS書き込みソフトウェアを作成できないようにできる。このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。

【0052】

この発明では、記録再生装置内で生成した暗号化鍵を記録再生装置自身がメディアへ書き込むことにより、CPRMのように、鍵情報を予め記録ディスクへ記録済みとする必要がなくなることから、ディスク製造にかかるコストの低下に貢献する。

【0053】

この発明では、PCと記録再生装置の相互認証時の乱数データにメディアタイプを含めることによって、セキュアにメディアタイプを記録再生装置からPCへ伝えることが可能となる。このことから、PCと記録再生装置間の標準化されたインターフェース上でのメディアタイプの改ざんや、改造された記録再生装置による成りすまし行為を防止することができる。

【0054】

この発明では、相互認証時の乱数データにコピー世代管理情報(CGMS)を含めることによって、セキュアにCGMSをPCから記録再生装置へ伝えることが可能となる。このことから、PCと記録再生装置間の標準化されたインターフェース上でのCGMSの改ざんや、改造されたPCアプリによる成りすまし行為を防止することができる。

【0055】

この発明では、相互認証が成立しない間は、暗号化鍵のディスクへの書き込みを記録再生装置内のエンコーダLSI(Large Scale Integrated Circuit:大規模集積回路)で禁止し、その暗号化鍵書き込み禁止機能を相互認証の成立によって解除することにより、一般のユーザによるCSS書き込みソフトウェアの作成を禁止できる。このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。

【発明を実施するための最良の形態】**【0056】**

以下、この発明について説明するが、この発明の理解を容易とするために、DVDレコーダでCSS方式による記録を実現するために、考えられるいくつかの例とその場合の問題点について説明する。また、以下の説明では、DVDメディアへの記録についてのみ説明し、再生処理については、CSS方式による再生処理と同様であるので、その説明を省略する。さらに、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

【0057】

記録媒体:メディア例えばDVDライタブルディスク、記録再生装置:ドライブ、情報処理装置:パーソナルコンピュータ、伝達手段:インターフェース、信号処理システム:メディアを記録再生するドライブとパーソナルコンピュータとがインターフェースを介して接続されるシステムである。

【0058】

コンテンツ情報:メディアに記録すべき情報例えばオーディオ/ビジュアルデータをコンテンツ情報としている。第1の暗号化鍵:マスターキーである。第2の暗号化鍵:ディスクキーであり、ディスク上には、暗号化されたセキュアドディスクキーとして記録される。第3の暗号化鍵:タイトルキーであり、ディスク上には、暗号化され、暗号化タイトルキーとして記録される。

【0059】

図8は、DVDレコーダ51aにおいて、記録型DVDメディア（以下、ライタブルまたはレコーダブルディスクと適宜称する）13aへCSS方式でコンテンツを書き込む際の記録方法の一例を示す。DVD-Videoと同様にライタブルディスク13aのリードインエリアの決められた場所に予めセキュアドディスクキー10aを書き込み済みとする例である。オーディオ/ビジュアルデータ60がDVDレコーダ51aのMPEGエンコーダ52によって圧縮符号化され、スクランブラ53によってスクランブルされ、スクランブルドMPEGデータ9がライタブルディスク13aに記録される。

【0060】

DVDレコーダ51aの内部の乱数生成器（RNG: Random Number Generator）54によりタイトルキーが生成される。タイトルキーは、記録の度に生成され、また、CGMSのステータスが変化した時にも生成される。スクランブラ53は、タイトルキーを使用してMPEGデータをスクランブルする。タイトルキーは、エンクリプタ55で暗号化され、ライタブルディスク13aに暗号化タイトルキー11が記録される。記録済みのセキュアドディスクキー10aがデクリプタ56において、マスターキー57によって復号され、ディスクキーが得られる。

【0061】

図9に示す例は、ライタブルディスクに暗号化鍵情報であるセキュアドディスクキーを予め書き込み済みとしない例である。DVDレコーダ51bが乱数発生器54および58を有し、乱数生成器54および58により、ディスクキーとタイトルキーを生成する。ディスクキーをDVDレコーダ51bがライタブルディスク13bに書き込む。例えばブランクディスクのフォーマッティングの処理によってディスクキーがライタブルディスク13bに対して書かれる。後からディスクキーを書き込むことによって、ディスクキーを書き込み済みとする図8の方法よりも記録型DVDメディアの製造コストを下げる事が可能となる。

【0062】

図10および図12にそれぞれ示す構成は、CSS方式でスクランブルされたビデオコンテンツを記録型DVDメディアへ書き込む機能を、PCとドライブの組み合わせで実現する場合の一例および他の例である。

【0063】

これらの図において、参照符号61がライタブルディスク13aまたは13bに対してデータを記録し、また、再生する記録再生装置としてのDVDドライブを示す。参照符号71がデータ処理装置（ホスト）としてのPCを示し、PC71に対してアプリケーションソフトウェアがインストールされ、DVDビデオエンコーダとしてPC71が機能する。但し、ソフトウェア処理に限定されるものではなく、DVDビデオエンコーダとしてハードウェア構成（基板構成）としても良い。

【0064】

DVDドライブ61とPC71との間がインターフェースで接続されている。インターフェースは、ATAPI (AT Attachment with Packet Interface), SCSI (Small Computer System Interface), USB (Universal Serial Bus), IEEE (Institute of Electrical and Electronics Engineers) 1394 等である。

【0065】

DVDドライブ61には、認証部62、バスエンクリプタ63およびバスデクリプタ64が備えられている。PC71には、認証部72、バスデクリプタ73およびバスエンクリプタ74が備えられている。また、PC71には、MPEGエンコーダ52、スクランブラ53、乱数発生器54、エンクリプタ55、デクリプタ56およびマスターキー57が備えられている。オーディオ/ビジュアルデータ60がMPEGエンコーダ52で、圧縮符号化され、DVDフォーマットの形式のストリームデータに変換される。スクランブラ53にてタイトルキーによってスクランブルされてDVDドライブ61にインターフェースを介して供給され、ライタブルディスク13a上にスクランブルドMPEGデータ9

が記録される。

【0066】

PC71の内部の乱数生成器54によりタイトルキーが生成される。スクランブラ53は、タイトルキーを使用してMP EGデータをスクランブルする。タイトルキーは、エンクリプタ55で暗号化され、認証が成立した時に生成されるセッションキーで暗号化タイトルキーがバスエンクリプタ74で暗号化される。バスエンクリプタ74の出力データがDVDドライブ61のバスデクリプタ64に供給され、バスデクリプタ64によってセッションキーで暗号化タイトルキーが復号される。ライタブルディスク13aに暗号化タイトルキー11が記録される。

【0067】

記録済みのセキュアドディスクキー10aがDVDドライブ61のバスエンクリプタ63において、認証の成立によって生成されたセッションキーによって暗号化される。DVDドライブ61からPC71へインターフェースを介して伝送され、バスデクリプタ73においてセッションキーを使用して復号される。さらに、デクリプタ56において、マスターキー57によって復号され、ディスクキーが取得される。

【0068】

図11は、図10に示すシステムにおいて、DVDドライブ61とPC71との間の信号の授受の手順を示す。PC71がDVDドライブ61に対してコマンドを送り、DVDドライブ61がコマンドに応答した動作を行う。ライタブルディスクの挿入等でシーケンスが開始し、最初に認証シーケンスAKE（ステップS21）がなされる。認証が成立すると、セッションキーKsをDVDドライブ61とPC71が共有する。認証が成立しなかった場合では、処理が中断する。

【0069】

次に、PC71からの要求に応じてDVDドライブ61がライタブルディスク13a上のコントロールデータゾーンを SEEK し、コントロールデータを読み出す（ステップS22）。次のステップS23において、PC71がセキュアドディスクキーを要求し、DVDドライブ61がセキュアドディスクキーをリードする（ステップS24およびS25）。DVDドライブ61がバスエンクリプタ63によってセッションキーKsでセキュアドディスクキーを暗号化し、暗号化されたセキュアドディスクキーをDVDドライブ61がPC71に送る（ステップS26）。PC71のバスデクリプタ73がセキュアドディスクキーを復号し、さらに、デクリプタ56によってディスクキーを復号する。

【0070】

次に、ステップS27において、DVDドライブ61が暗号化タイトルキーおよびCGMSをバスエンクリプタ74において、セッションキーKsで暗号化し、DVDドライブ61に対して送出する。さらに、ステップS28において、スクランブラ53からのスクランブルドMP EGデータがDVDドライブ61に送出される。DVDドライブ61は、バスデクリプタ6においてセッションキーKsで復号した暗号化タイトルキーと、スクランブルドMP EGデータをライタブルディスク13a上に記録する（ステップS29）。

【0071】

図12に示す構成例は、図10と比較すると、ライタブルディスク13bに対してセキュアドディスクキーを記録する点で相違している。このため、乱数発生器58がPC71に備えられ、ディスクキーが生成される。ディスクキーがエンクリプタ59において、マスターキー57によって暗号化され、セキュアドディスクキーがバスエンクリプタ75において、セッションキーKsによって暗号化される。バスエンクリプタ75の出力がDVDドライブ61にインターフェースを介して伝送され、バスデクリプタ65において、セッションキーKsによって復号される。そして、ライタブルディスク13b上にセキュアドディスクキー10bが記録される。他の構成は、図10に示すシステムと同様である。

【0072】

図13は、図12に示すシステムにおけるDVDドライブ61とPC71との間の信号の授受の手順を示す。前述した図10のシステムにおける図11に示される手順と同様で

ある。但し、バスエンクリプタ 75 において、セッションキー Ks で暗号化されたセキュアドディスクキーが DVD ドライブ 61 に対して送出され (ステップ S33)、DVD ドライブ 61 がバスデクリプタ 65 によってセッションキー Ks で復号したセキュアドディスクキーをライタブルディスクに対してライトする処理 (ステップ S34) が相違している。

【0073】

上述した図 10 および図 12 に示す構成または方法を採用すると、一般ユーザが自作した CSS 書き込みソフトウェアを使って作成した CSS 暗号化データイメージを、通常のライトコマンドで書き込むことが可能という欠陥がある。理由は、CSS 方式のアルゴリズムは秘密とは言えず、公知とされていることによる。図 10 の例であれば、認証が成立した時点でアプリケーションソフトウェアを自作のものに切り替え、また、ライタブルディスク 13a に予め記録されたセキュアドディスクキーに合わせて、自ら生成したタイトルキーを利用してコンテンツをスクランブルする CSS スクランブラを CSS 契約を受けない者が作成することが可能である。

【0074】

次に、さらなる構成例について説明する。上述した図 10 および図 12 に示す構成または方法では、スクランブルド MPEG データが DVD ドライブ 61 と PC 71 間の ATA PI 等の標準化されたインターフェースを通るために、書き込み中のスクランブルド MPEG データが横から盗まれ、これに「DeCSS」を施すことで平文に戻すという行為がなされる危険性がある。この点を考慮してスクランブルド MPEG データに対してもバス暗号化および復号を施すものが図 14 および図 16 にそれぞれ示す構成例である。

【0075】

図 14 の構成例は、予めライタブルディスク 13a 上にセキュアドディスクキー 10a が記録されている点は、図 10 のシステムと同様である。図 10 のシステムと相違する点は、スクランブラ 53 の出力に得られるスクランブルド MPEG データがバスエンクリプタ 76 によって暗号化されてから DVD ドライブ 61 にインターフェースを介して伝送され、DVD ドライブ 61 において、バスデクリプタ 66 によって復号されることである。これによって、インターフェースを通る時にスクランブルド MPEG データが横取りされるおそれを少なくできる。

【0076】

図 15 は、図 14 のシステムにおける DVD ドライブ 61 と PC 71 との間の信号の授受の手順を示す。この手順は、図 10 のシステムの手順を示す図 11 と同様のものである。相違する点は、ステップ S28 において、スクランブルド MPEG データを送る処理がステップ S38 のセッションキー Ks で暗号化されたスクランブルド MPEG データを送ることに変わっていることである。

【0077】

図 16 の構成例は、ライタブルディスク 13b 上にセキュアドディスクキー 10b を記録する点は、図 12 のシステムと同様である。図 12 のシステムと相違する点は、スクランブラ 53 の出力に得られるスクランブルド MPEG データがバスエンクリプタ 76 によって暗号化されてから DVD ドライブ 61 に伝送され、DVD ドライブ 61 において、バスデクリプタ 66 によって復号されることである。これによって、インターフェースを通る時にスクランブルド MPEG データが横取りされるおそれを少なくできる。例えば放送コンテンツから得られたスクランブルド MPEG データを横取りしてハードディスクに記録し、その後「DeCSS」でもって復号することがされるおそれがある。

【0078】

図 17 は、図 16 のシステムにおける DVD ドライブ 61 と PC 71 との間の信号の授受の手順を示す。この手順は、図 12 のシステムの手順を示す図 13 と同様のものである。相違する点は、ステップ S28 において、スクランブルド MPEG データを送る処理がステップ S38 のセッションキー Ks で暗号化されたスクランブルド MPEG データを送ることに変わっていることである。

【0079】

上述した図14および図16に示すさらなる構成または方法においても、一般ユーザが自作したCSS書き込みソフトウェアを使って作成したCSS暗号化データイメージを、通常のライトコマンドで書き込むことが可能という欠陥がある。

【0080】

このように、ライタブルディスクに対する書き込みにCSSを適用する場合に生じる問題を、この発明は、解決することができる。以下、図面を参照してこの発明のいくつかの実施形態について説明する。

【0081】

図18は、この発明の第1の実施形態のシステム構成例を示す。参照符号161がDVDドライブを示し、参照符号171がDVDドライブ161と標準的なインターフェースで接続され、ホストとして機能する情報処理装置例えばPCである。PC171に対してアプリケーションソフトウェアがインストールされ、またはハードウェア（基板）が備えられることによって、PC171がDVDビデオエンコーダとして機能する。例えばテレビジョンチューナの基板に対してハードウェアのビデオエンコーダ基板が組み込まれる構成とされる。第1の実施形態では、予めリードインエリアにセキュアドディスクキー10aが記録されているライタブルディスク13aが使用される。例えばライタブルディスクとしては、DVD+R/RW、またはDVD-R/RWを使用できる。

【0082】

DVDドライブ161は、タイトルキーを生成する乱数発生器81と、生成したタイトルキーをディスクキーで暗号化するエンクリプタ82と、マスターキー83と、セキュアドディスクキーをマスターキーで復号するデクリプタ84とを内部に備えている。さらに、認証部62、セッションキーKsでセキュアドディスクキーを暗号化するバスエンクリプタ63、スクランブルDMPEGデータを復号するバスデクリプタ66が備えられている。かかるDVDドライブ161は、CSS鍵発行センターの正規の承認を得てこれらの構成要素を備えたものである。また、DVDドライブ161は、ハードウェア（LSI）で構成されているので、信号処理の内容を外部から知ることが不可能な耐タンパー性を有している。

【0083】

ライタブルディスク13aから読まれたセキュアドディスクキー10aがデクリプタ84においてマスターキー83によって復号され、ディスクキーがエンクリプタ82に供給される。エンクリプタ82において、乱数発生器81からのタイトルキーが暗号化され、暗号化タイトルキーが生成される。暗号化タイトルキーがCSS方式で規定されているようにライタブルディスク13aに対して記録される。

【0084】

アプリケーションソフトウェアまたはハードウェア（基板）によってDVDビデオエンコーダとしての機能をPC171が有する。DVDドライブ161の認証部62およびPC171の認証部72の相互認証が成立すると、セッションキーKsが生成される。DVDドライブ161のバスエンクリプタ63において、セッションキーKsによってセキュアドディスクキーが暗号化され、バスエンクリプタ85において、セッションキーKsによって暗号化タイトルキーが暗号化される。これらの暗号化されたデータが標準的なインターフェースを介してPC171に伝送される。

【0085】

PC171では、バスデクリプタ73において、セッションキーKsによってセキュアドディスクキーが復号され、バスデクリプタ77において、セッションキーKsによって暗号化タイトルキーが復号される。デクリプタ56において、マスターキー57によってディスクキーが復号され、デクリプタ78において、バスデクリプタ77からの暗号化タイトルキーがディスクキーによって復号され、タイトルキーが得られる。

【0086】

オーディオ/ビジュアルデータ60がMPPEGエンコーダ52において、MPPEG2に

よって圧縮符号化されると共に、DVD規格のフォーマットのデータへ変換される。例えばMPEGエンコーダ52では、デジタル放送等で受信されたトランスポートストリームがプログラムストリームへ変換され、DVDフォーマットのデータへ変換される。MPEGエンコーダ52の出力データがスクランブラ53にてタイトルキーによってスクランブルされる。スクランブラ53からのスクランブルドMPEGデータがバスエンクリプタ76において、セッションキーKsによって暗号化される。バスエンクリプタ76の出力データがインターフェースを介してDVDドライブ161に伝送される。DVDドライブ161では、バスデクリプタ66によってスクランブルドMPEGデータが復号され、スクランブルドMPEGデータがライタブルディスク13aに記録される。なお、PC171において、MPEGエンコーダ52以外の構成要素は、CSS鍵発行センターの正規の承認を得て備えたものである。

【0087】

図19は、図18に示すシステムにおいて、DVDドライブ161とPC171との間の信号の授受の手順を示す。PC171がDVDドライブ161に対してコマンドを送り、DVDドライブ161がコマンドに応答した動作を行う。ライタブルディスクの挿入等でシーケンスが開始し、最初に認証シーケンスAKE（ステップS41）がなされる。認証が成立すると、セッションキーKsをDVDドライブ161とPC171が共有する。認証が成立しなかった場合では、処理が中断する。

【0088】

次に、PC171からの要求に応じてDVDドライブ161がライタブルディスク13a上のコントロールデータゾーンをシークし、コントロールデータを読み出す（ステップS42）。次のステップS43において、PC171がセキュアドディスクキーを要求し、DVDドライブ161がセキュアドディスクキーをリードする（ステップS44およびS45）。DVDドライブ161がバスエンクリプタ63によってセッションキーKsでセキュアドディスクキーを暗号化し、暗号化されたセキュアドディスクキーをDVDドライブ161がPC171に送る（ステップS46）。PC171のバスデクリプタ73がセッションキーKsによってセキュアドディスクキーを復号し、さらに、デクリプタ56によってディスクキーを復号する。

【0089】

次に、ステップS47において、認証シーケンスAKEがなされる。認証が成立すると、セッションキーKsが新たに生成され、このセッションキーKsをDVDドライブ161とPC171が共有する。認証が成立しなかった場合では、処理が中断する。認証が成立すると、ステップS48において、PC171がCGMSをDVDドライブ161に対して送る。ステップS49において、PC171がDVDドライブ161に対してセッションキーKsで暗号化されたタイトルキーを要求する。

【0090】

DVDドライブ161は、エンクリプタ82からの暗号化タイトルキーをエンクリプタ85に供給し、セッションキーKsで暗号化タイトルキーを暗号化する。このエンクリプタ85からのKsで暗号化された暗号化タイトルキーをPC171に対して戻す（ステップS50）。

【0091】

PC171では、バスデクリプタ77および78による復号処理によってタイトルキーを生成し、スクランブラ53において、MPEGデータを暗号化し、スクランブルドMPEGデータを生成する。さらに、スクランブルドMPEGデータをバスエンクリプタ76においてセッションキーKsで暗号化し、Ksで暗号化されたスクランブルドMPEGデータをDVDドライブ161に伝送する（ステップS51）。DVDドライブ161は、バスデクリプタ66においてセッションキーKsで受け取ったデータを復号してスクランブルドMPEGデータを得る。そして、スクランブルドMPEGデータと暗号化タイトルキーをライタブルディスク13a上にライトする（ステップS52）。

【0092】

上述した第1の実施形態は、ドライブ161内で生成したタイトルキーをセキュアにPC171へ転送してPC側でのCSSスクランブルに利用し、PC171から受け取ったCSSスクランブルMPEGデータとドライブ161で生成したタイトルキーをライタブルディスク13aへ書き込む方法である。したがって、第1の実施形態は、PC側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでCSSスクランブルをさせないことができ、ライセンスを受けないものが自由にCSSスクランブル書き込みソフトウェアを作ることを防止することができる。

【0093】

図20は、この発明の第2の実施形態のシステム構成を示す。第2の実施形態は、ライタブルディスク13bに対してセキュアドディスクキーを記録するものである。DVDドライブ161は、タイトルキー生成用の乱数発生器81に加えて、ディスクキー生成用の乱数発生器86が設けられている。ディスクキーがタイトルキーをエンクリプタ82において暗号化するために使用される。また、ディスクキーがマスターキー83によってエンクリプタ87で暗号化され、セキュアドディスクキーが生成される。セキュアドディスクキー10bがライタブルディスク13b上のリードインエリアに記録される。

【0094】

このように、ディスクキーを生成し、生成したディスクキーを暗号化してセキュアドディスクキーを生成し、セキュアドディスクキー10bをリードインエリアに記録することを除くと、第2の実施形態の構成および処理は、図18に示す第1の実施形態のものと同様である。

【0095】

図21は、図20に示すシステムにおいて、DVDドライブ161とPC171との間の信号の授受の手順を示す。図21に示されるものは、図19に示す信号の授受の手順と同様である。相違する点は、セキュアドディスクキーをPC171が要求した時に、DVDドライブ161がセキュアドディスクキーをライタブルディスク13bに記録するステップS54と、このセキュアドディスクキーをセッションキーKsで暗号化してPC171に戻す点である。

【0096】

第2の実施形態は、ドライブ161内で生成したディスクキーとタイトルキーをセキュアにPC171へ転送してPC側ビデオエンコーダーでのCSSスクランブルに利用し、PC171から受け取ったスクランブルドMPEGデータと、ドライブ161で生成したセキュアドディスクキーと、暗号化タイトルキーをライタブルディスクへ書き込む方法である。かかる第2の実施形態は、PC側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでCSSスクランブルをさせないことから、ライセンスを受けないものが自由にCSSスクランブル書き込みソフトウェアを作ることを防止する効果がある。さらに、DVDメディアへ予めディスクキーを記録しておく必要がないことから、メディアの製造コストを低くすることができる。

【0097】

図22を参照して第3の実施形態について説明する。第3の実施形態では、ライタブルディスク13aのリードインエリアに予めセキュアドディスクキーが記録されている。セキュアドディスクキー10aは、マスターキー83によってデクリプタ84において復号され、ディスクキーが得られる。タイトルキーは、DVDドライブ261内の乱数発生器81によって生成され、エンクリプタ82でディスクキーによって暗号化される。エンクリプタ82からの暗号化タイトルキー11がライタブルディスク13a上に記録される。

【0098】

DVDドライブ261は、認証部91を有し、PC271の認証部92と相互認証を行う。認証が成立するとセッションキーKsをDVDドライブ261とPC271とが共有する。この相互認証の方法は、CSS方式と同様のものに限らず、後述するような新たな方法を採用できる。新たな認証方法を採用することによって、ライセンスを受けないものによるCSS書き込みソフト作成をより確実に防ぐことが可能となる。

【0099】

PC271は、認証部92を有する以外には、オーディオ／ビジュアルデータ60を符号化するMP EGエンコーダ52とバスエンクリプタ93とを有するのみである。その他の処理は、DVDドライブ261においてなされる。PC271は、CSSスクランブルするための一切の鍵や処理を持たず、相互認証機能を持つのみであり、負荷が著しく軽くなる。

【0100】

DVDドライブ261は、PC271からのセッションキーKsで暗号化されたMP EGデータをバスデクリプタ94においてセッションキーKsで復号する。そして、スクランブラ95で暗号化し、スクランブルドMP EGデータ9をライタブルディスク13a上に記録する。スクランブラ95は、乱数発生器81によって生成されたタイトルキーによってMP EGデータを暗号化し、スクランブルドMP EGデータを生成する。

【0101】

第3の実施形態も、PC側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでCSSスクランブルをさせないことから、ライセンスを受けないものが自由にCSSスクランブル書き込みソフトウェアを作ること防止する効果がある。新たな認証方法を導入すれば、ライセンスを受けない者によって書き込みソフトウェアが作成されることをより確実に防止できる。さらに、PC側の負荷を軽くすることができる。

【0102】

図23は、第4の実施形態を示す。第3の実施形態と相違する点は、DVDドライブ261の乱数発生器86によってディスクキーを生成し、ディスクキーをエンクリプタ87においてマスターキー83によって暗号化し、セキュアドディスクキー10bをライタブルディスク13bに対して記録することである。第3の実施形態と同様に、PC271が認証部92と、バスエンクリプタ93と、MP EGエンコーダ52を有する。

【0103】

かかる第4の実施形態も上述した第3の実施形態と同様の作用効果を奏するものである。さらに、DVDメディアへ予めディスクキーを記録しておく必要がないことから、メディアの製造コストを低くすることができる。

【0104】

図24は、図18に示す第1の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール101を加えた第5の実施形態を示す。マスクコントロール101に対してエンクリプタ82からの暗号化タイトルキーが入力され、マスクコントロール101の出力に取り出された暗号化タイトルキー11がライタブルディスク13a上に記録される。

【0105】

マスクコントロール101は、DVDドライブ161の認証部62の認証の結果に応答してマスク機能が制御される。すなわち、PC171とDVDドライブ161の相互認証が成立し、セッションキーKsが生成されている間はマスク機能が解除され、暗号化タイトルキー11がライタブルディスク13a上に記録される。一方、認証が成立しなければマスク機能は有効となり、暗号化タイトルキー11が無効データまたはダミーデータ例えばゼロデータに置き換えられ、暗号化タイトルキーのライタブルディスク13a上への書き込みが実質的に禁止される。

【0106】

図25は、図20に示す第2の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール101と、セキュアドディスクキーのマスク制御機構としてのマスクコントロール102とを加えた第6の実施形態を示す。マスクコントロール101と同様に、マスクコントロール102は、セキュアドディスクキーに対してマスク機能を発揮する。すなわち、PC171とDVDドライブ161の相互認証が成立し、セッションキーKsが生成されている間はマスク機能が解除され、セキュアドディスクキー10bがライタブルディスク13b上に記録される。一方、認証が成立しなければマス

ク機能は有効となり、セキュアドディスクキー10bがライタブルディスク13b上に記録されない。

【0107】

上述した第5および第6の実施形態のように、ディスクへのCSSキーの書き込みを相互認証の成立結果によって制御することによって、一般のユーザによるCSS書き込みソフトウェアの作成をより確実に禁止することが可能となる。それによって正規に許可された者だけがCSS書き込みアプリケーションソフトウェアを作成することができる。

【0108】

図26は、図22に示す第3の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール103を加えた第7の実施形態を示す。マスクコントロール103に対してエンクリプタ82からの暗号化タイトルキーが入力され、マスクコントロール103の出力に取り出された暗号化タイトルキー11がライタブルディスク13a上に記録される。

【0109】

マスクコントロール103は、DVDドライブ161の認証部62の認証の結果に応答してマスク機能が制御される。すなわち、PC171とDVDドライブ161の相互認証が成立し、セッションキーKsが生成されている間はマスク機能が解除され、暗号化タイトルキー11がライタブルディスク13a上に記録される。一方、認証が成立しなければマスク機能は有効となり、暗号化タイトルキー11がライタブルディスク13a上に記録されない。

【0110】

図27は、図23に示す第4の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール103と、セキュアドディスクキーのマスク制御機構としてのマスクコントロール104とを加えた第8の実施形態を示す。マスクコントロール103と同様に、マスクコントロール104は、セキュアドディスクキーに対してマスク機能を発揮する。すなわち、PC171とDVDドライブ161の相互認証が成立し、セッションキーKsが生成されている間はマスク機能が解除され、セキュアドディスクキー10bがライタブルディスク13b上に記録される。一方、認証が成立しなければマスク機能は有効となり、セキュアドディスクキー10bがライタブルディスク13b上に記録されない。

【0111】

上述した第7および第8の実施形態のように、ディスクへのCSSキーの書き込みを相互認証の成立結果によって制御することによって、一般のユーザによるCSS書き込みソフトウェアの作成をより確実に禁止することが可能となる。それによって正規に許可された者だけがCSS書き込みアプリケーションソフトウェアを作成することができる。

【0112】

図28は、上述した第3の実施形態(図22)、第4の実施形態(図23)、第7の実施形態(図26)および第8の実施形態(図27)のそれぞれに備えられている認証部91および92に適用される認証構成または方法の一例を説明するものである。図28に示す例では、相互認証からセッションキーを生成すると同時に、ディスクタイプの情報をセキュアにドライブからPCへ伝えるようにしている。ディスクタイプデータは、下記のように定義された2ビットの情報である。

【0113】

(0, 0) : ROM (0, 1) : 未定義 (1, 0) : ライタブル タイプ1
(1, 1) : ライタブルディスク タイプ2

例えばタイプ1は、リライタブルディスクを示し、タイプ2は、1回のみ記録可能なディスクを示す。他の例としては、タイプ1がCSS方式の書き込みが許されている種類のディスクを意味し、タイプ2がCSS方式の書き込みが許されていない種類のディスクを意味する。ディスクタイプは、ディスク上のリードインエリア内の所定位置に記録されている。但し、ウォプリンググループの情報に記録されているものであっても良く、また、

ディスクの光学的特性から判定されたものでも良い。図28において、参照符号301がディスクタイプデータを示す。

【0114】

ディスクタイプデータ301がマルチプレクサ302および303にそれぞれ供給され、乱数発生器304および305からの乱数と混合され、ディスクタイプデータを含む64ビットの乱数データRa1およびRa2がそれぞれ生成される。例えば64ビットの乱数中の所定の2ビットのビット位置例えば下位側の2ビットにディスクタイプデータが配置される。この乱数Ra1およびRa2がPC側に伝送され、デマルチプレクサ401によって乱数Ra1からディスクタイプデータ301をPCが得ることができる。PCは、取得したディスクタイプのデータに対応するアプリケーションソフトウェアを実行する。

【0115】

DVDドライブ161の認証部91は、認証キーKmを有する。認証キーKmは、多くの場合にLSI内部に配置され、外部から読み出すことができないようセキュアに記憶される。ドライブ161がCSSによる記録を扱う正当なドライブとなるためには、認証キーKmのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成が防止される。

【0116】

参照符号306、307および308は、認証キーKmをパラメータとしてMAC値を計算するMAC(Message Authentication Code)演算ブロックをそれぞれ示す。また、参照符号304、305および309が64ビットの乱数を発生する乱数発生器である。上述したように、ディスクタイプと乱数とがマルチプレクサ302で合成されてマルチプレクサ302から乱数Ra1が出力され、この乱数Ra1がMAC演算ブロック306に供給される。マルチプレクサ303からの乱数Ra2がMAC演算ブロック307に供給される。さらに、乱数発生器309が乱数Ra3を生成する。乱数発生器304、305、309は、例えばLSIの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数Ra1、Ra2、Ra3は、互いに独立したものである。

【0117】

PC側の認証部92も、認証キーKmを有し、認証キーKmをパラメータとしてMAC値を計算するMAC演算ブロック406、407および408を備えている。さらに、それぞれ64ビットの乱数Rb1、Rb2、Rb3をそれぞれ発生する乱数発生器404、405および409が備えられている。乱数28 Rb1、Rb2、Rb3は、PC側の認証部92のMAC演算ブロック406、407および408にそれぞれ供給されると共に、DVDドライブ側に伝送され、MAC演算ブロック306、307、308に対して供給される。乱数発生器404、405、409は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

【0118】

DVDドライブの認証部91において生成された乱数と、PCの認証部92において生成された乱数とが交換される。すなわち、乱数Ra1および乱数Rb1がMAC演算ブロック306および406に入力され、乱数Ra2および乱数Rb2がMAC演算ブロック307および407に入力され、乱数Ra3および乱数Rb3がMAC演算ブロック308および408に入力される。

【0119】

MAC演算ブロック306が演算したMAC値と、MAC演算ブロック406が演算したMAC値とが認証部92内の比較410において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $eKm(Ra1 \parallel Rb1)$ と表記される。 $eKm()$ は、認証キーKmを鍵として括弧内のデータを暗号化することを表している。 $Ra1 \parallel Rb1$ の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、PCによるDVDドライブの認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【0120】

MAC演算ブロック307が演算したMAC値と、MAC演算ブロック407が演算したMAC値とがドライブの認証部91内の比較310において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、eKm(Rb2 || Ra2)と表記される。比較の結果、二つの値が同一と判定されると、DVDドライブによるPCの認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【0121】

かかる相互認証において、比較310および410の両者において、MAC値が同一と判定され、DVDドライブおよびPCの両者の正当性が確認されると、すなわち、相互認証が成功すると、MAC演算ブロック308および408によって、共通のセッションキーeKm(Ra3 || Rb3)がそれぞれ生成される。このように、互いのMAC計算値を交換して一致確認をすることから、途中の経路での改ざんや互いのなりすましを防ぐことが可能となる。なお、この発明では、相互認証に限らず、片方向の認証のみを行うようにしても良い。

【0122】

ディスクタイプデータの他の例を下記に示す。

【0123】

(0, 0) : ROM (0, 1) : 未定義 (通常書き込み可能) (1, 0) : 未定義 (通常書き込み可能) (1, 1) : ビデオライタブルディスク (CSS/CPRMによるビデオ記録が可能で、私的録画補償金がディスク販売価格に含まれているディスク)

【0124】

このように定義されたディスクタイプデータが上述したようにPC側に伝送される乱数に混合した場合に、ドライブ側の処理およびPC側の処理の一例を説明する。図29は、ドライブ側の処理を示すフローチャートである。

【0125】

冒頭に挙げた非特許文献3に記載されているように、ディスク上には、ウォブリングしたグループが予め形成されている。ウォブリングは、ADIP (Address in Pre-groove) と称される情報によって変調されたものである。ADIPに含まれる情報の一つがメディアタイプ (3バイト) である。最初のステップST101において、メディアタイプが判別される。判別結果がROMか否かがステップST102において判定される。ROMであれば、ステップST103において、ディスクタイプがROM (0, 0) と判定される。ROMでない場合には、ステップST104において、ディスクアプリケーションコードがビデオライタブルか否かが判定される。

【0126】

ADIPに含まれる情報の他のものがディスクアプリケーションコード (1バイト) である。ディスクアプリケーションコードは、特別のアプリケーションにのみ使用されるように制限されたディスクであるか否かを識別するのに使用される。例えばディスクアプリケーションコードによって、ビデオ信号を書き込むことが可能なこと (ビデオライタブル) が識別される。

【0127】

ステップST104において、ディスクアプリケーションコードがビデオライタブルであれば、ディスクタイプがビデオライタブルと判定される (ステップST106)。若し、ステップST104において、ディスクアプリケーションコードがビデオライタブルでないと判定されると、ディスクタイプがリザーブド (すなわち、未定義) と判定される (ステップST105)。

【0128】

このようにドライブが判定したディスクタイプが上述したように、相互認証時に交換される乱数に混合されたPC側へ伝送される。図30は、PC側の処理を示すフローチャートである。ステップST111において、相互認証がなされ、ステップST112におい

て、PCがドライブからディスクタイプデータを取得する。

【0129】

ディスクタイプがROMがどうかステップST113において判定される。ROMと判定されると、ステップST114において、データの書き込みが禁止される。ROMでないと判定されると、ステップST115において、ディスクタイプがビデオライタブルか否かが判定される。ビデオライタブルでないと判定されると、ステップST116において、データ書き込みが可能と判定される。ビデオライタブルであると判定されると、ステップST117において、CSS/CPRMによる書き込み可能と判定される。

【0130】

図31は、認証部91および92の他の例を示す。他の例は、上述した一例が相互認証に加えて、ディスクタイプの情報をDVDドライブからPCへ伝える機能を有するのに対して、CGMSの情報をPCからDVDに伝えるものである。

【0131】

PC9の認証部92には、記録しようとするCGMSデータ411が存在する。CGMSデータ411は、記録すべきビデオデータに含まれる著作権管理情報に基づいた2ビットのデータであり、以下のように定義された2ビットの情報である。

【0132】

(0, 0) : コピーフリー (0, 1) : EPN (Encryption Plus Non-assertion) (デジタル放送におけるコンテンツ管理情報) (1, 0) : 1回のコピーのみ許可 (1, 1) : コピー禁止

CGMSデータ411は、記録しようとするビデオ入力から分離されたものである。例えば分離されたCGMSデータが(1, 0)で1回のコピーのみ許可されている場合では、ライタブルディスクに記録されるCGMSデータは、1回コピーがされた結果、(1, 1)のコピー禁止に変更される。

【0133】

PC側の認証部92において、CGMSデータ411がマルチプレクサ412および413にそれぞれ供給され、乱数発生器404および405からの乱数と混合され、CGMSデータを含む64ビットの乱数データRb1およびRb2がそれぞれ生成される。例えば64ビットの乱数中の所定の2ビットのビット位置例えば下位側の2ビットにCGMSデータが配置される。この乱数Rb1およびRb2がDVDドライブ側に伝送され、デマルチプレクサ311によって乱数Rb2からCGMSデータ411をDVDドライブが得ることができ、CGMSデータ411がライタブルディスク上の所定の位置に記録される。

【0134】

図32は、MAC演算ブロック306, 307, 308, 406, 407, 408として、AES (Advanced Encryption Standard) エンクリプタを使用した場合の構成例を示す。二つの乱数AおよびBを結合した128ビットの乱数A || Bと認証キーKmとがAESエンコーダに供給され、認証キーKmを鍵として乱数A || Bを暗号化した出力eKm(A || B)が形成される。

【0135】

さらに、図28に示す構成の場合における相互認証の処理の流れを図33および図34のフローチャートを参照して説明する。図33のフローチャートは、DVDドライブ側の認証部91の処理の流れを示し、図34は、PC側の認証部92の処理の流れを示す。最初に、図34中のステップST21において、コマンドSEND KEYにより、認証部91に対して乱数発生器404および405でそれぞれ生成された乱数Rb1と乱数Rb2が転送される。図33中のステップST11において、認証部91が認証部92から転送されたこれらの乱数を受け取る。

【0136】

その後、認証部92は、コマンドREPORT KEYにより認証部91に対して認証キーKmを鍵としたMACによるレスポンス値と乱数Ra1 (ディスクタイプデータを含む) とを認証部92へ転送することを要求する (ステップST22)。このレスポンス値は、eKm(Ra1

|| Rb1)と表記される。eKm () は、認証キーKmを暗号鍵として括弧内のデータを暗号化することを表している。Ra1 || Rb1の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。

【0137】

認証部92からコマンドREPORT KEYを受け取った認証部91は、ステップST12において、MAC演算ブロック306が生成したMAC値eKm(Ra1 || Rb1)と乱数Ra1を認証部92へ転送する。ステップST23において、認証部92は、自身のMAC演算ブロック406でMAC値を計算し、比較410において認証部91から受け取った値と一致するかを確認を行う。若し、受け取ったMAC値と計算されたMAC値とが一致すれば、認証部92(PC)による認証部91(DVDドライブ)の認証が成功したことになる。ステップST23における比較の結果が同一でない場合には、認証部92(PC)による認証部91(DVDドライブ)の認証が失敗したことになり、リジェクト処理がなされる。

【0138】

認証部92による認証部91の認証が成功した場合には、ステップST24において、認証部92が認証部91へコマンドREPORT KEYを送付し、認証部91から乱数Ra2(ディスクタイプデータを含む)と乱数Ra3の転送を要求する。このコマンドに応答して、ステップST13において、認証部91は、これらの乱数を認証部92へ転送する。

【0139】

ステップST25において、認証部92のMAC演算ブロック407は、認証部91から受け取った乱数から認証部92が持つ認証キーKmを鍵としたMACによるレスポンス値eKm(Rb2 || Ra2)を計算し、乱数Rb3とともに、コマンドSEND KEYを用いて認証部91へ転送する。

【0140】

ステップST14において、認証部91は、認証部92からレスポンス値eKm(Rb2 || Ra2)および乱数Rb3を受け取ると、自身でMAC値を計算し、ステップST15において、比較310によって認証部92から受け取ったMAC値と一致するかを確認を行う。若し、受け取ったMAC値と計算されたMAC値とが一致すれば、認証部91(DVDドライブ)による認証部92(PC)の認証が成功したことになる。この場合には、ステップST16において、MAC演算ブロック308がセッションキーeKm(Ra3 || Rb3)を生成し、また、認証部92に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

【0141】

ステップST15における比較の結果が同一でない場合には、認証部91による認証部92の認証が失敗したことになり、ステップST17において、認証が失敗したことを示すエラー情報が認証部92に送信される。

【0142】

認証部92は、送付したコマンドSEND KEYに対する応答として認証部91から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップST26において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップST27において、MAC演算ブロック408がドライブ側と共通のセッションキーeKm(Ra3 || Rb3)(例えば64ビット長)を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。

【0143】

上述したこの発明の全ての実施形態においては、PCからDVDドライブへ伝送される記録データをバスエンクリプタで暗号化し、DVDドライブでは、バスデクリプタで復号している。図35において、参照符号501がバスエンクリプタを示し、参照符号511がバスデクリプタを示す。

【0144】

PCからDVDドライブに対しては、2KB(キロバイト)のセクタデータからなるパ

ックでもってデータが伝送される。パックは、パックヘッダによってパックの種類が指定されている。A Vパック検出部 5 0 2 は、オーディオパック、ビデオパックおよびサブピクチャパックを検出し、検出結果に応じて制御信号を出力する。

【0145】

A Vパック検出部 5 0 2 からの制御信号によってセクタ 5 0 3 が制御される。入力データがオーディオパック、ビデオパックおよびサブピクチャパックの場合には、入力データを A Vデータエンクリプタ 5 0 4 に導き、セッションキーによって暗号化する。但し、パックヘッダは、暗号化されない。また、これらのパック以外の場合では、入力データを暗号化しないで、インターフェースを介して DVDドライブに伝送する。

【0146】

バスデクリプタ 5 1 1 の A Vパック検出部 5 1 2 において、受け取ったパックの種類をパックヘッダから検出する。セクタ 5 1 3 が A Vパック検出部 5 1 2 からの制御信号で制御される。パックがオーディオパック、ビデオパックおよびサブピクチャパックの場合には、受取データを A Vデータデクリプタ 5 1 4 に導き、セッションキーによって復号する。

【0147】

C S S方式で保護の対象となるのは、オーディオ／ビジュアルデータであるので、コンピュータのファイルデータ等の他の一般的データを暗号化する必要がない。そのために、A Vパックのみを暗号化している。

【0148】

図 3 6 は、バス暗号化／復号の処理の流れを示す。ステップ S T 3 1 において、パックヘッダ検出部の検出結果からビデオパックか否かが判定される。ビデオパックであれば、ステップ S T 3 2 において、データが暗号化／復号される。ビデオパックでなければ、ステップ S T 3 3 のオーディオパックか否かの判定ステップに処理が移る。

【0149】

ステップ S T 3 3 において、オーディオパックと判定されれば、ステップ S T 3 2 においてデータが暗号化／復号され、そうでないと判定されれば、ステップ S T 3 4 のサブピクチャパックか否かの判定ステップに処理が移る。ステップ S T 3 4 において、サブピクチャパックと判定されれば、ステップ S T 3 2 においてデータが暗号化／復号され、そうでないと判定されれば、データを暗号化／復号しない（ステップ S T 3 5）。そして、バス暗号化／復号の処理が終了する。

【0150】

図 3 7 は、DVDビデオデータのオーディオパック、ビデオパックまたはサブピクチャパックの構成を示す。パックの制御情報が配置されたパックヘッダが先頭に配置され、その後にパケットヘッダが配置され、その後にオーディオデータ（A C 3 データ）、ビデオデータ（M P E G プログラムストリーム）またはサブピクチャデータ（字幕等のテキストデータ）が配置される。パックヘッダおよびパケットヘッダは、可変長データであるので、これらのデータ長が最も長い場合を考慮して、パックヘッダおよびパケットヘッダを含む例えば 1 2 8 バイトがバス暗号化／復号の対象外とされ、残りの 1 9 2 0 バイトがバス暗号化／復号の対象とされる。合計の 2 K（2 0 4 8）バイトが 1 セクタのメインデータとされる。

【0151】

上述した第 5 の実施形態（図 2 4）、第 6 の実施形態（図 2 5）、第 7 の実施形態（図 2 6）および第 8 の実施形態（図 2 7）では、DVDドライブと P C との相互認証が成立したか否かに応じて制御されるマスクコントロール 1 0 1、1 0 2、1 0 3、1 0 4 を設けている。これらのマスクコントロールのマスクの対象とするデータについて説明する。最初にライタブルディスクに記録されるデータの構成について説明する。

【0152】

DVDドライブでは、P C から受け取ったデータをセクタ構造に変化してライタブルディスクに記録する。図 3 8 は、1 セクタのデータ構成を示す。2 K バイトのメインデータ

に対して12バイトのセクタヘッダが付加され、また、最後の4バイトがセクタ全体の対するエラー検出コードEDCとされ、全体で2064バイトのデータセクタが構成されている。

【0153】

セクタヘッダの先頭の4バイトがセクタ番号等のIDであり、その後の2バイトがIDに対するエラー検出用コードIEDであり、その後の6バイトがコピー管理用データCPR__MAI(Copyright Management Information)である。CPR__MAIは、コピー管理(著作権管理)が必要なデータがメインデータとして記録される場合に必要データである。CPR__MAI内にメインデータを復号するのに必要な暗号化タイトルキーが配置されている。

【0154】

図38に示すセクタ構造のデータを記録時に生成する処理を図39を参照して説明する。図39に示すように、セクタヘッダのIDが用意される。このIDは、DVDドライブ内のCPUによって生成される。すなわち、記録時にPCからライトコマンドがDVDドライブに対して伝送され、書き込みコマンドにディスクへの記録位置を示すLBA(Logical Block Address)データと、ライトデータ長のデータが付加されている。DVDドライブのCPUは、ライトコマンドの指示内容が実行可能であると判断すると、ライトデータ長の分だけ、PCからドライブのバッファメモリに対して2Kバイトのバック単位でデータを伝送させて蓄える。

【0155】

そして、実際にライト動作を開始する前に、LBAデータからディスク上の物理的アドレスであるPSN(Physical Sector Number)を計算し、その値をIDとする。そのIDに対してエラー検出コードIEDが付加され、ID+IED(6バイト)が形成される。

【0156】

さらに、(ID+IED)データに対してCPR__MAIおよびメインデータが付加され、さらに、これらのデータからセクタ毎のエラー検出符号EDCが生成され(ステップST41)、スクランブルされる前の1単位(1フレーム)のデータが形成され、その1単位のデータ内のメインデータに対してタイトルキーでスクランブルが施され、スクランブルドメインデータを含むフレームが形成される(ステップST42)。

【0157】

さらに、スクランブルが施されたフレームを16フレーム集めたデータに対してエラー訂正符号化を行う(ステップST43)。エラー訂正符号化で生成されたECCが付加された16フレームのデータ内のメインデータに対してインターリーブ処理が施される(ステップST44)。そして、セクタ毎に26シンクフレームを変調する(ステップST45)。変調処理後のデータがライタブルディスクに記録される。

【0158】

図40は、6バイトのCPR__MAIのより詳細なデータ構成を示す。図40Aは、(PSN<030000h)のリードインエリア内のCPR__MAIのデータ構成を示し、図38Bは、(PSN≥030000h)のデータエリア内のCPR__MAIのデータ構成を示す。図40Aに示すリードインエリア内のCPR__MAIは、一種の属性情報であり、書かれているデータがセキュアドディスクキーであることを示す情報が含まれている。先頭の1バイトBP0が著作権保護システムタイプを示す。例えば著作権保護システムタイプがCSS対応か否か、並びにCPRM対応のものか否かが示される。

【0159】

次のバイトBP1は、セキュアドディスクキーモードである。次のバイトBP2およびBP3は、未定義である。次のバイトBP4の上位の2ビットが未定義とされ、下位の6ビットがビデオ認証コントロールコードとされる。さらに、バイトBP5が地域(リージョン)管理情報とされている。

【0160】

図40Aにおいて破線で囲んで示すように、リードインエリア内のCPR__MAIの全

てのデータがマスクの対象とされる。すなわち、認証が成立しないでマスクを行う時には、リードインエリア内のCPR_MAIの全てのデータが例えば00hのデータに書き換えられる。ビデオ認証コントロールコードは必ずしもマスクしないでも良い。

【0161】

図40Bに示すデータエリア内のCPR_MAIについて説明すると、先頭のバイトBP0にCPM(1ビット)、CP_SEC(1ビット)、CGMS(2ビット)、CPS_MOD(4ビット)が配置されている。そして、残りの5バイトBP1~BP5に対して暗号化ビデオタイトルキーが上位側から下位側に向かって順に配置されている。

【0162】

図40Bにおいて破線で囲んで示すように、データエリア内のCPR_MAIの内の先頭バイトBP0以外のバイトBP1~BP5(暗号化ビデオタイトルキー)がマスクの対象とされる。すなわち、認証が成立しないでマスクを行う時には、リードインエリア内のCPR_MAIのバイトBP1~BP5が例えば00hのデータに書き換えられる。

【0163】

図41は、データエリア内のCPR_MAIに対するマスクコントロールの構成の一例を示す。この例では、図39に示される記録処理において、EDCを加えるステップST41の直前でマスクコントロールを行うようにしている。図41において、参照符号601がセクタ情報(1バイト)が蓄えられているレジスタであり、参照符号602がPSN(3バイト)が蓄えられているレジスタである。これらの4バイトのIDが演算部603に入力され、2バイトのエラー検出符号IEDが算出される。

【0164】

参照符号604は、CPR_MAIの先頭の1バイトBP0が蓄えられているレジスタである。参照符号605は、メインデータ(2Kバイト)が蓄えられているバッファメモリである。CPR_MAIの1バイトBP0がCPR_MAIフィルタ606に入力され、所定のPSNでCPR_MAIがフィルタリングされて取り出される。6バイトのCPR_MAIの先頭の1バイトBP0が演算部607に入力され、他の5バイトが全てゼロのデータとされて演算部607に入力される。演算部607によってセクタ全体のエラー検出符号EDCが生成される。参照符号608で示すミキサーに対してセクタ情報、PSN、エラー検出コードIED、CPR_MAI、メインデータ、EDCが入力され、図38に示す構成の1セクタのデータが構成される。

【0165】

図42は、CPR_MAIフィルタ606の一例を示す。ディスク上のアドレスであるPSN(3バイト)が比較器611に入力され、所定のアドレス例えば030000hと比較される。また、CPR_MAIの先頭の1バイトBP0がセクタ612の一方の入力端子に供給される。セクタ612の他方の入力端子には、全てゼロのデータ00hが入力されている。セクタ612は、比較器611の出力によって制御される。セクタ612の出力にマスクコントロールされたCPR_MAIが取り出される。

【0166】

比較器611において、(PSN<030000h)と判定されると、リードインエリアに記録されるCPR_MAI(図40A参照)と決定され、セクタ612がBP0を00hのデータへ置き換える。これ以外では、比較器611の出力によって、BP0をセクタ612が選択して出力する。

【0167】

図43は、セッションキーの生成および消滅と、CSSキー(暗号化タイトルキーおよびセキュアドディスクキー、または暗号化タイトルキー)のマスク制御の処理の流れを示すフローチャートである。最初のステップST51では、この発明の対象とするCSSスクランブル書き込みが許可されたディスク例えばDVD+RW/+Rディスクが挿入されたか否かが判定される。ディスクが挿入されたと判定されると、ステップST52においてPCアプリケーションが起動されているか否かが判定される。すなわち、PCが電源オン、あるいは再起動を経て、OSが起動しPCからアプリケーションプログラムの実行が

可能か否かが判定される。CSSキー書き込みマスク機能は、デフォルトで書き込みを禁止する状態にある。なお、ステップST51およびST52の順序は、逆であっても良い。

【0168】

PCアプリケーションが起動されていると、ステップST52で判定されると、ステップST53において、相互認証がなされ、セッションキーが生成される。セッションキーの生成が完了したか否かがステップST54において判定され、若し、完了したと判定されると、CSSキーの書き込みマスク機能が解除される（ステップST55）。

【0169】

ステップST56において、PCアプリケーションが終了したか否かが判定される。PCアプリケーションが終了したと判定されると、ステップST57において、PC内で生成されたセッションキーが消去される（ステップST57）。そして、PCアプリケーションが再び起動されているかどうか判定される（ステップST58）。起動されていると判定されると、ステップST53に制御が戻る。

【0170】

ステップST58において、アプリケーションが起動されていないと判定されると、DVDRW/+Rディスクが排出されたか否かがステップST59において判定される。排出されていないと判定されると、制御がステップST58に戻る。ディスクが排出されたらステップST59において判定されると、ステップST60において、ドライブ内で生成したセッションキーが消去される。そして、マスクコントロールによってCSSキー書き込みが禁止される（ステップST61）。

【0171】

ステップST56において、アプリケーションが起動されていないと判定されると、DVDRW/+Rディスクが排出されたか否かがステップST62において判定される。排出されていないと判定されると、制御がステップST56に戻る。ディスクが排出されたらステップST62において判定されると、ステップST63において、ドライブ内で生成したセッションキーが消去される。そして、マスクコントロールによってCSSキー書き込みが禁止される（ステップST61）。

【0172】

なお、マスターキーの配信構成を特開2002-236622号公報に記載されているようなツリー構造を使用しても良い。図44は、図26に示す実施の形態に対してこの方法を適用した場合の構成を示す。ドライブ261には、複数のドライブで共通のデバイスノードキー111およびドライブ固有のデバイスID112を保持する。また、ライタブルディスク13aには、EKB (Enable Key Block) 14と呼ばれるブロックデータによって構成されるテーブルが格納されている。EKBには、複数の暗号化キーが含まれる。

【0173】

ライタブルディスクからEKBが復号部113に読み込まれ、復号部113において、デバイスノードキー111と、デバイスID112とによってマスターキーが復号される。この方法は、新たなマスターキーの配布、或いはマスターキーの更新に利用することができる。

【0174】

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばマスターキー、ディスクキーおよびタイトルキーの3つの暗号化鍵を使用する暗号化方法であれば、CSS方式以外の暗号化方法を使用しても良い。また、この発明は、ディスク以外に光カード、メモリカード等の媒体に対して情報を記録する場合に対しても適用することができる。

【図面の簡単な説明】

【0175】

【図1】 CSS方式でROMディスクへ記録する際の鍵情報の関係を示すブロック図である。

【図2】CSS方式で記録されたROMディスクを再生するDVDプレーヤー内の鍵情報とスクランブルデータの再生の方法を示すブロック図である。

【図3】ROMディスクのリードインエリアのデータ構成を示す略線図である。

【図4】セクタの構成を示す略線図である。

【図5】CSS方式によるコピー防止機能を説明するための略線図である。

【図6】CSS方式で記録されたROMディスクを再生するPCとドライブでの鍵情報とスクランブルデータの再生の方法を示すブロック図である。

【図7】図6のシステムにおけるドライブとディスク間のデータの流れを示す略線図である。

【図8】ディスクキーが書き込み済みの記録型DVDメディアへCSS方式でデータを書き込む際の記録方法の一例を示すブロック図である。

【図9】ディスクキーが書き込み済みでない記録型DVDメディアへCSS方式でデータを書き込む際の記録方法の一例を示すブロック図である。

【図10】ディスクキーが書き込み済みの記録型DVDメディアへCSS方式でデータを書き込む際の記録方法をPCとドライブの組み合わせで実現する場合の一例を示すブロック図である。

【図11】図10の構成におけるドライブとディスク間のデータの流れを示す略線図である。

【図12】ディスクキーが書き込み済みでない記録型DVDメディアへCSS方式でデータを書き込む際の記録方法をPCとドライブの組み合わせで実現する場合の一例を示すブロック図である。

【図13】図12の構成におけるドライブとディスク間のデータの流れを示す略線図である。

【図14】図10の構成に対してスクランブルデータをバス暗号化して転送するようにした構成を示すブロック図である。

【図15】図14の構成におけるドライブとディスク間のデータの流れを示す略線図である。

【図16】図12の構成に対してスクランブルデータをバス暗号化して転送するようにした構成を示すブロック図である。

【図17】図16の構成におけるドライブとディスク間のデータの流れを示す略線図である。

【図18】この発明の第1の実施形態の構成を示すブロック図である。

【図19】図18の構成におけるドライブとディスク間のデータの流れを示す略線図である。

【図20】この発明の第2の実施形態の構成を示すブロック図である。

【図21】図20の構成におけるドライブとディスク間のデータの流れを示す略線図である。

【図22】この発明の第3の実施形態の構成を示すブロック図である。

【図23】この発明の第4の実施形態の構成を示すブロック図である。

【図24】図18の構成に対してタイトルキーのマスク制御機構を加えたこの発明の第5の実施形態の構成を示すブロック図である。

【図25】図20の構成に対してディスクキーとタイトルキーのマスク制御機構を加えたこの発明の第6の実施形態の構成を示すブロック図である。

【図26】図22の構成に対してタイトルキーのマスク制御機構を加えたこの発明の第7の実施形態の構成を示すブロック図である。

【図27】図23の構成に対してディスクキーとタイトルキーのマスク制御機構を加えたこの発明の第8の実施形態の構成を示すブロック図である。

【図28】相互認証からセッションキーを生成する仕組みを示しており、同時にディスクタイプをセキュアにドライブからPCへ伝える仕組みを説明する略線図である。

【図29】ドライブ側におけるディスクタイプの情報の処理を説明するフローチャー

トである。

【図30】PC側におけるディスクタイプの情報の処理を説明するフローチャートである。

【図31】相互認証からセッションキーを生成する仕組みを示しており、同時にコピー世代管理情報をセキュアにドライブからPCへ伝える手段を説明する略線図である。

【図32】MAC計算やセッションキー生成においてAESを利用した場合の例を示すブロック図である。

【図33】相互認証からセッションキー生成までのドライブ側の処理を示すフローチャートである。

【図34】相互認証からセッションキー生成までのPC側の処理を示すフローチャートである。

【図35】バス暗号化／復号の処理の一例を示すブロック図である。

【図36】図35の処理の流れを示すフローチャートである。

【図37】AVパックの構造とバス暗号化の対象範囲を説明するための略線図である。

【図38】1セクタのデータ構成を示す略線図である。

【図39】データの記録処理の流れを示す略線図である。

【図40】マスクコントロールが対象とするデータを説明するための略線図である。

【図41】マスクコントロールの構成の一例を示すブロック図である。

【図42】マスクコントロール内のフィルタの構成の一例を示すブロック図である。

【図43】セッションキーの生成と消滅、およびCSSキーのマスクコントロールの処理を示すフローチャートである。

【図44】マスターキーの生成方法の他の例を示すブロック図である。

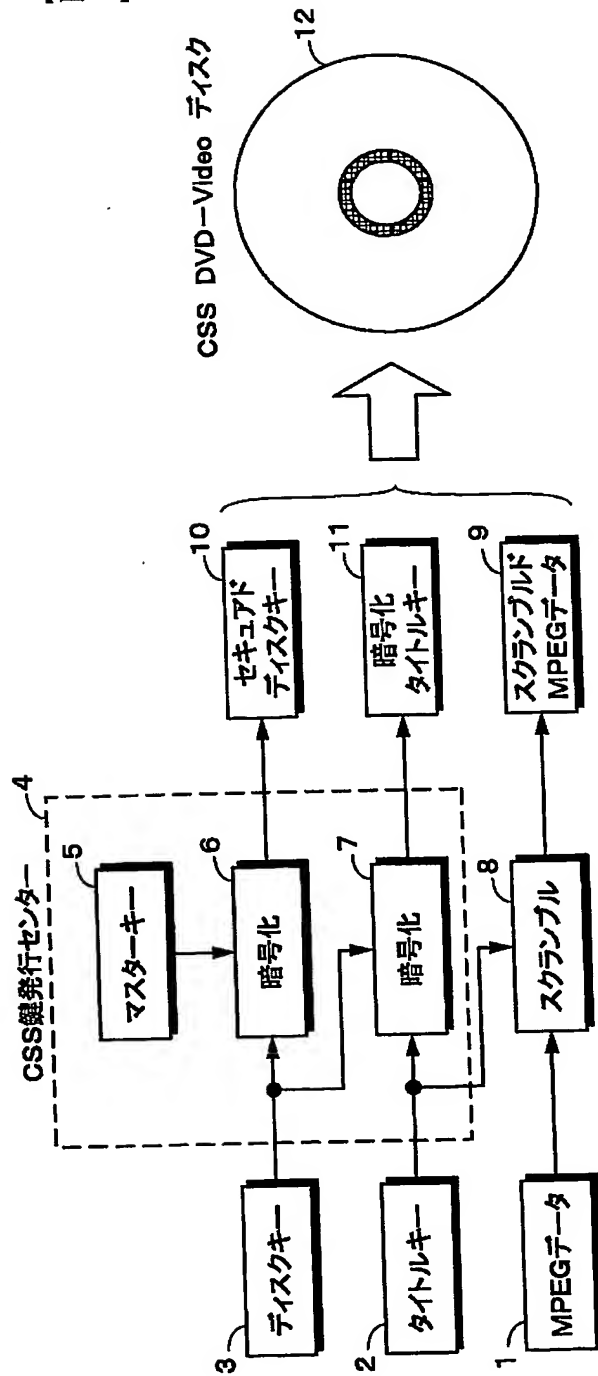
【符号の説明】

【0176】

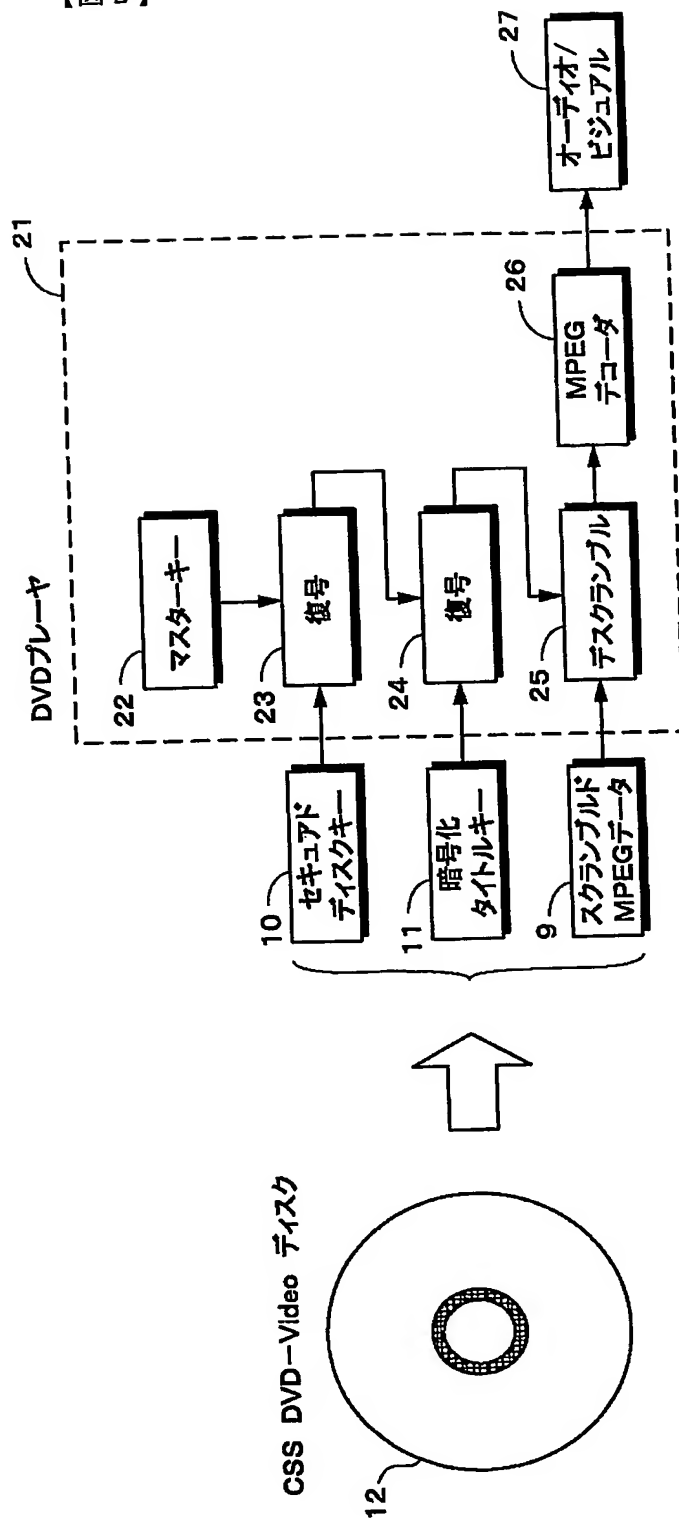
9	スクランブルDMPEGデータ
10a, 10b	セキュアドディスクキー
11	暗号化タイトルキー
13a, 13b	ライタブルディスク
52	MPEGエンコーダ
53, 95	スクランブラ
56, 78, 84	デクリプタ
57, 83	マスターキー
60	オーディオ／ビジュアルデータ
62, 72	認証部
63, 76, 85	バスエンクリプタ
66, 73, 77	バスデクリプタ
81, 86	乱数発生器
82, 87	エンクリプタ
161, 261	ドライブ
171, 271	PC

【書類名】 図面

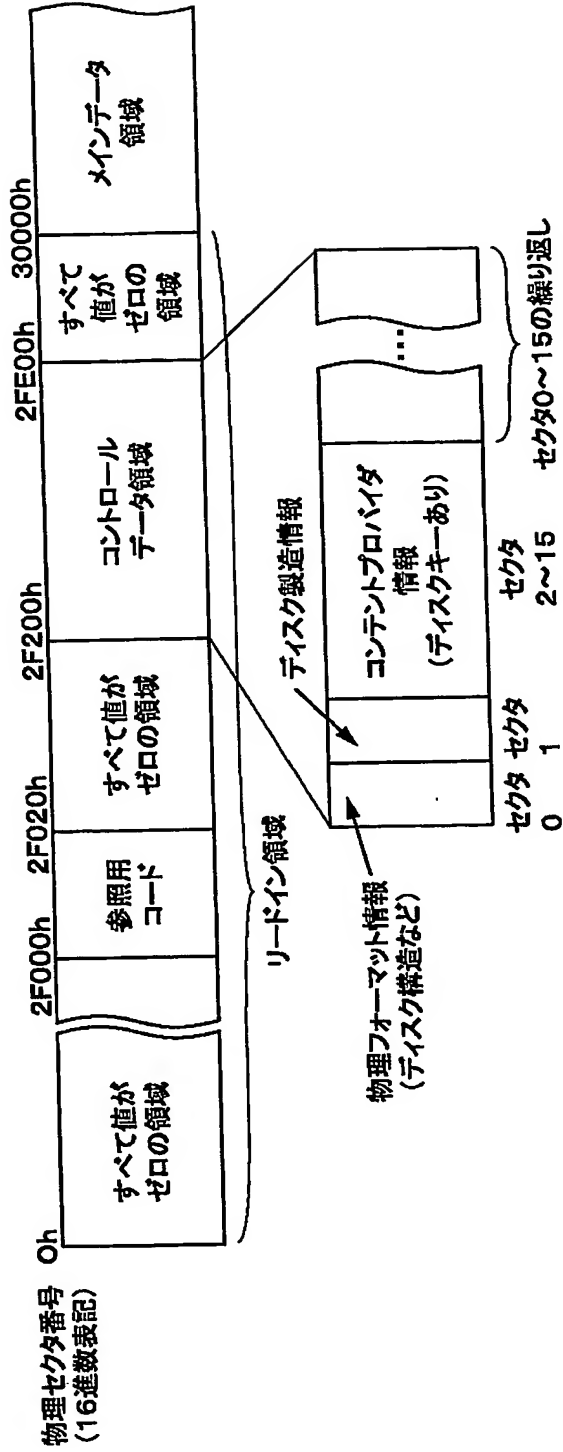
【図 1】



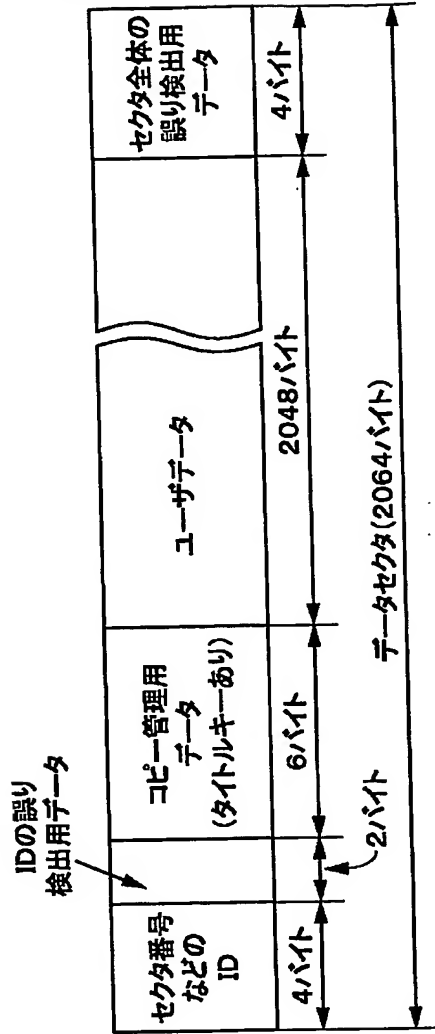
【図 2】



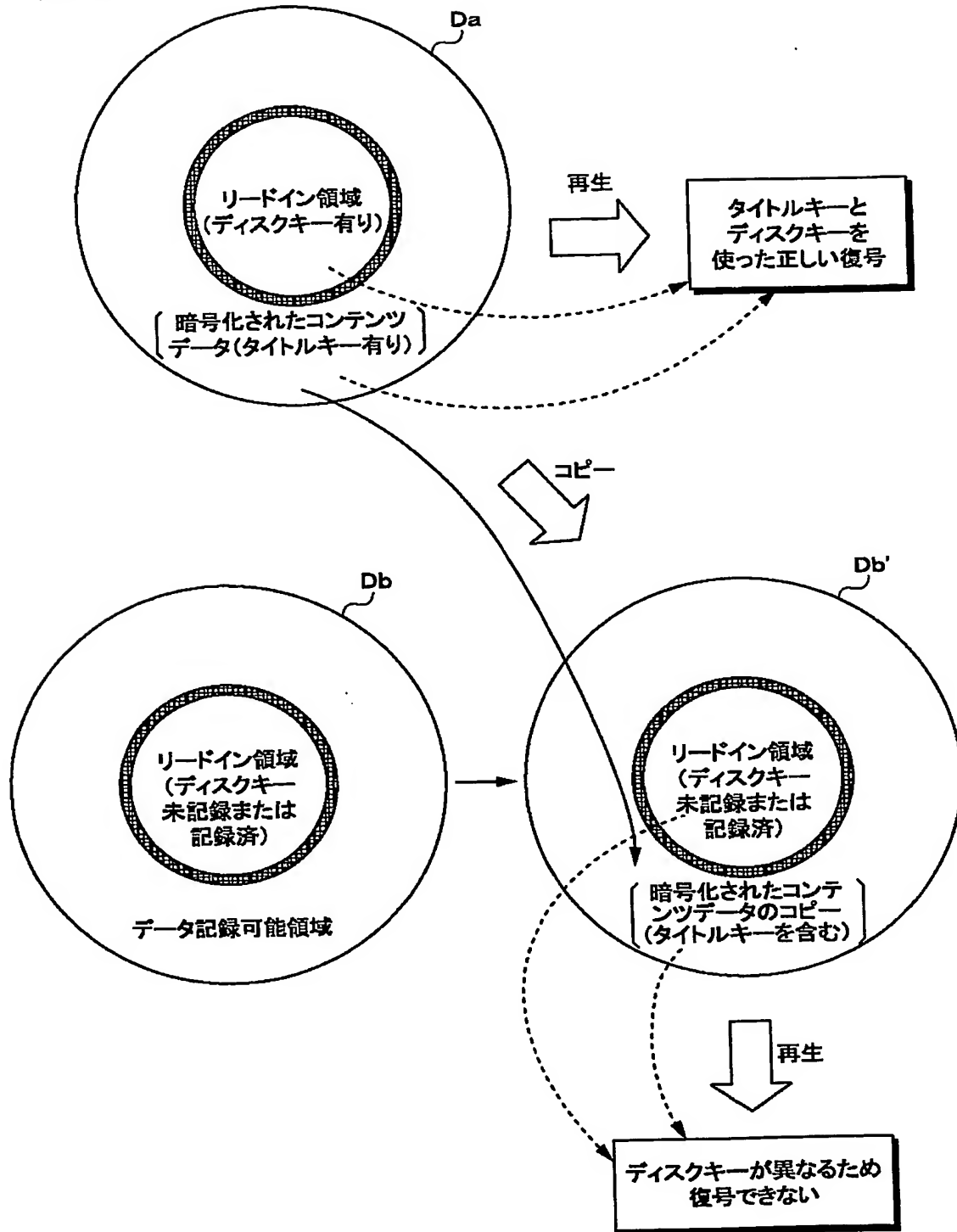
【図 3】



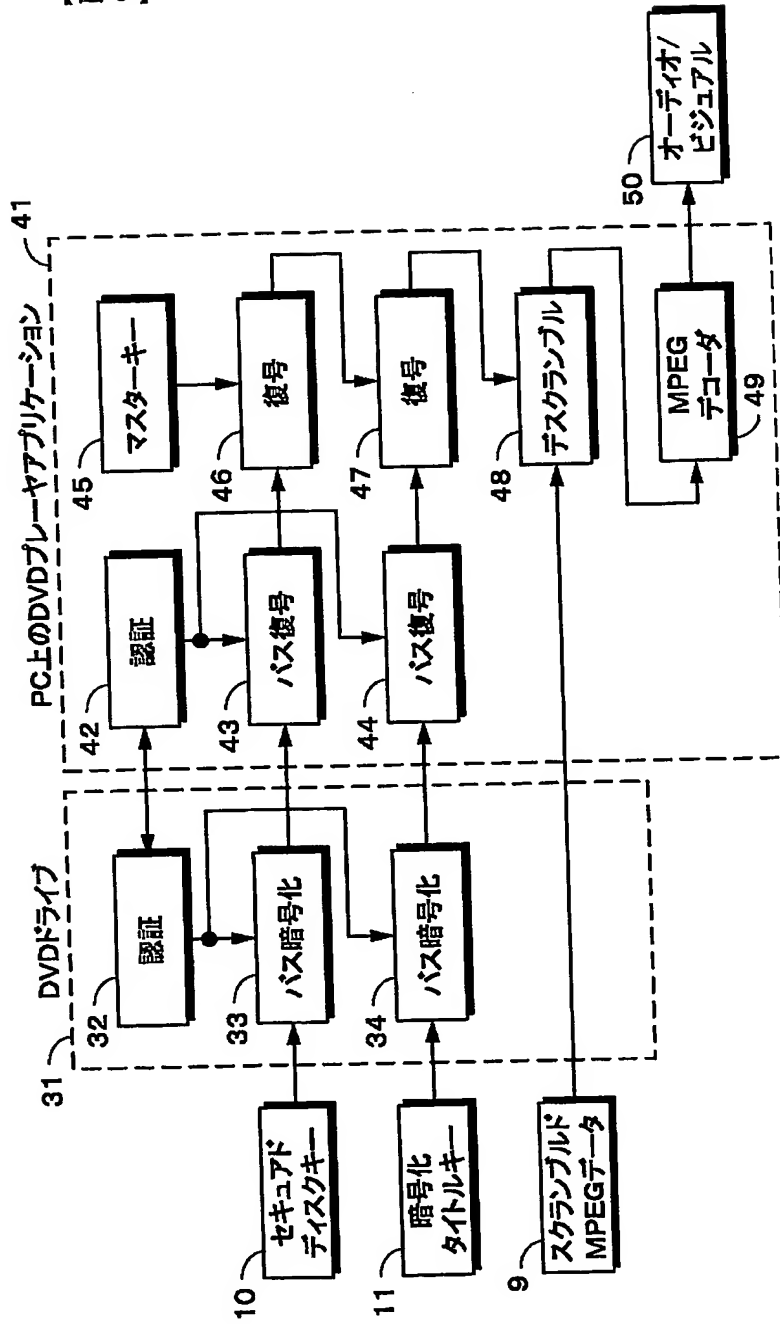
【図 4】



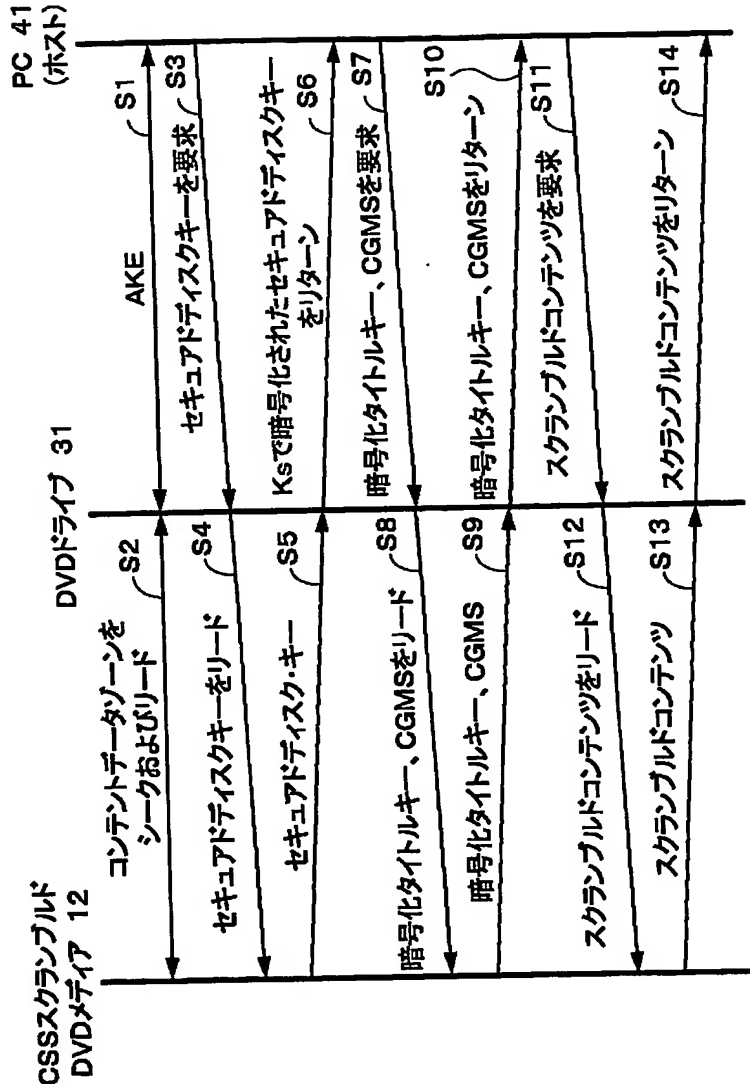
【図 5】



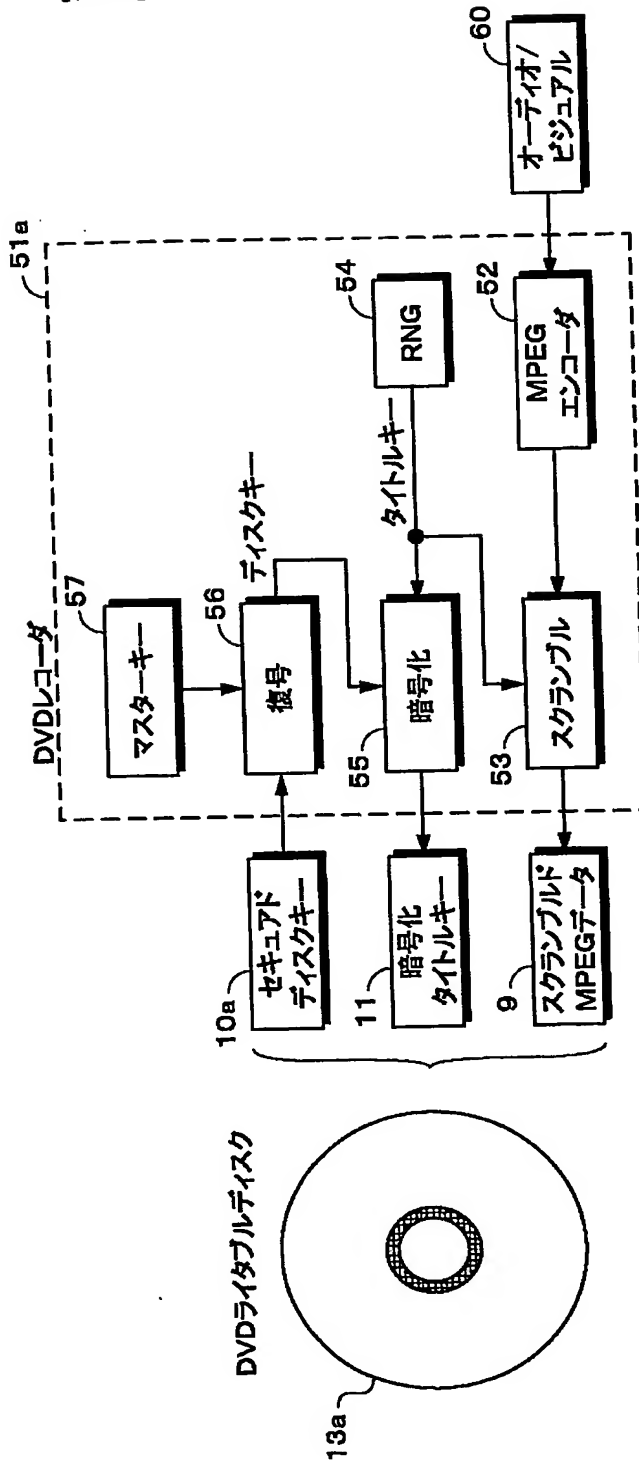
【図 6】



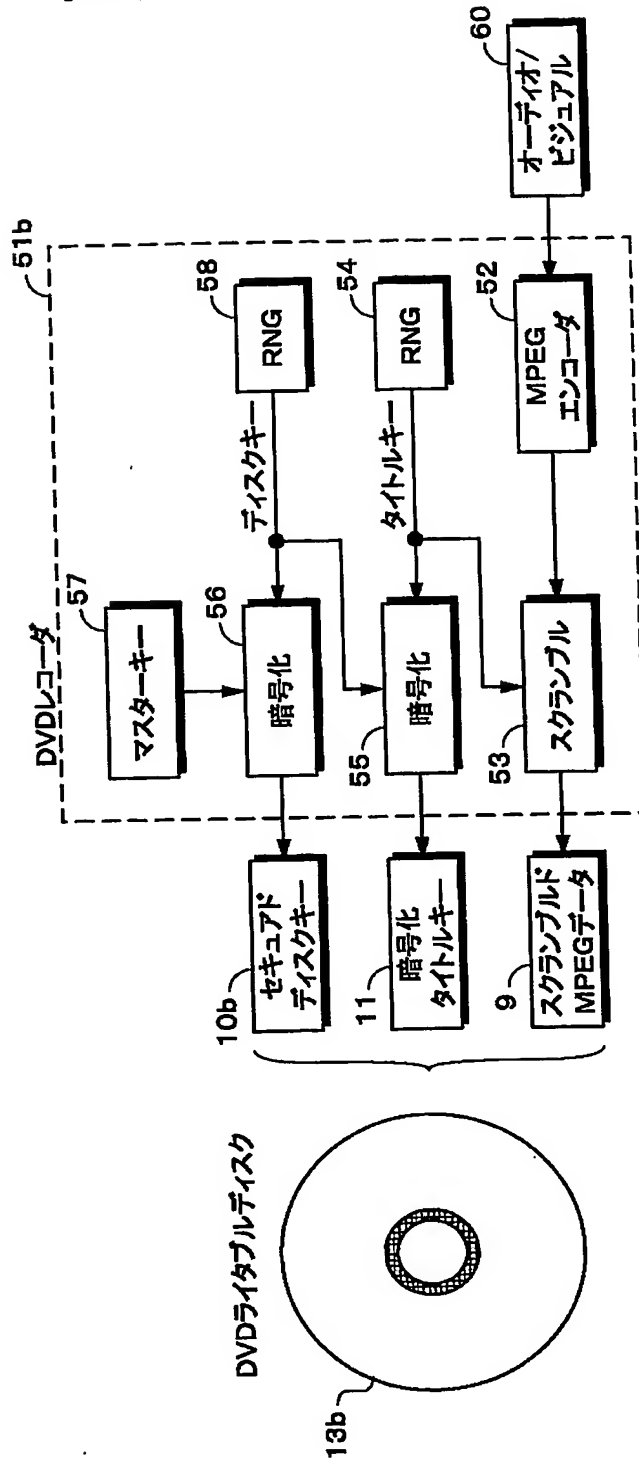
【図7】



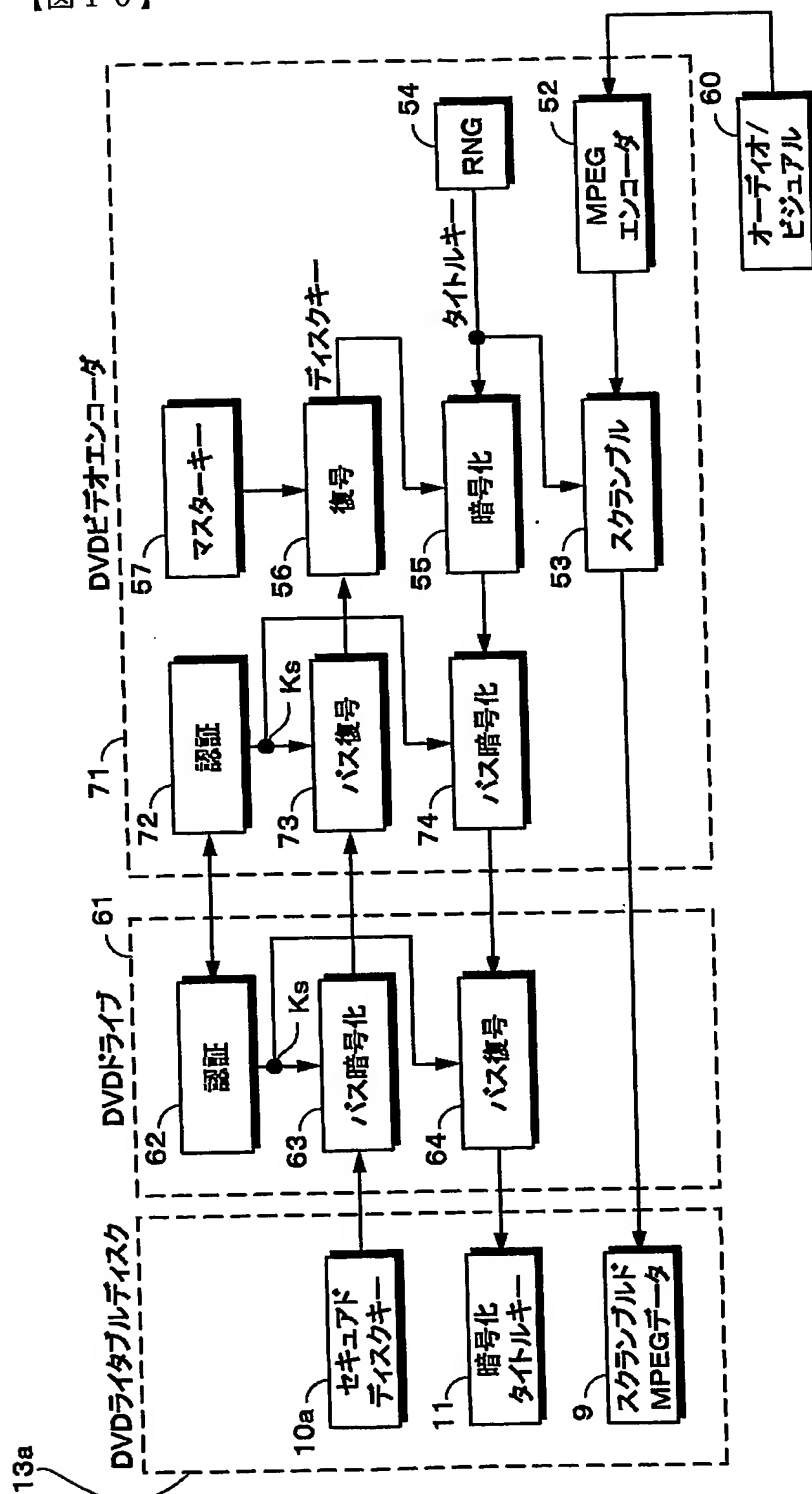
【図 8】



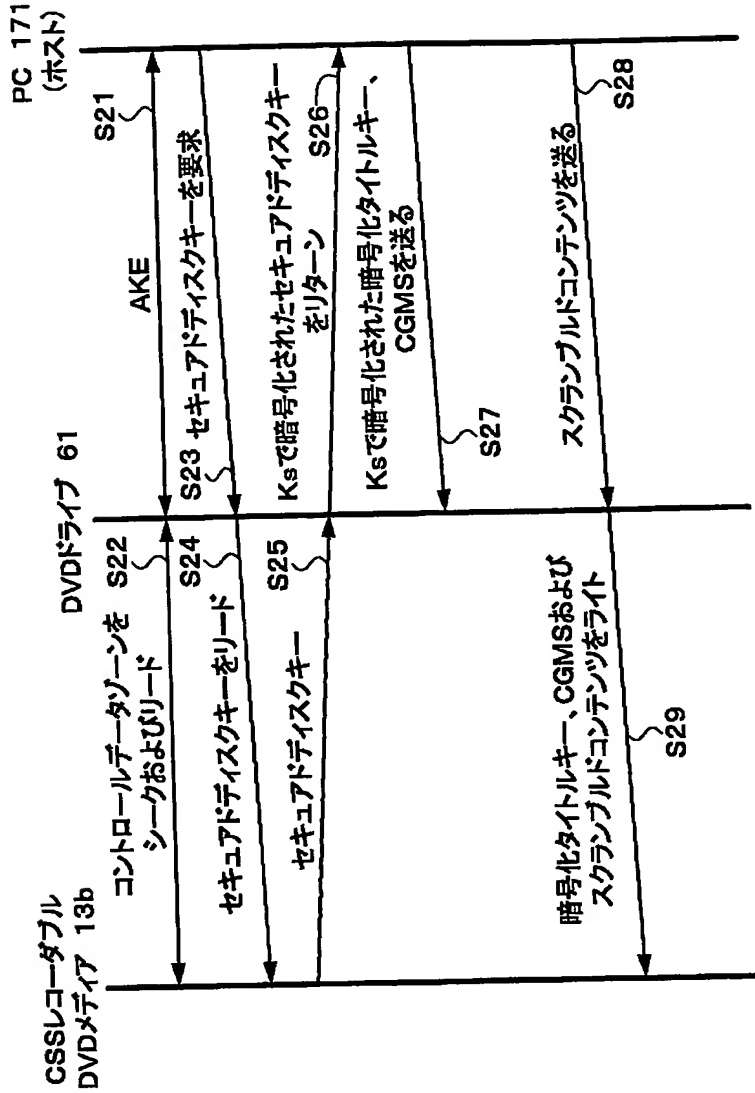
【図 9】



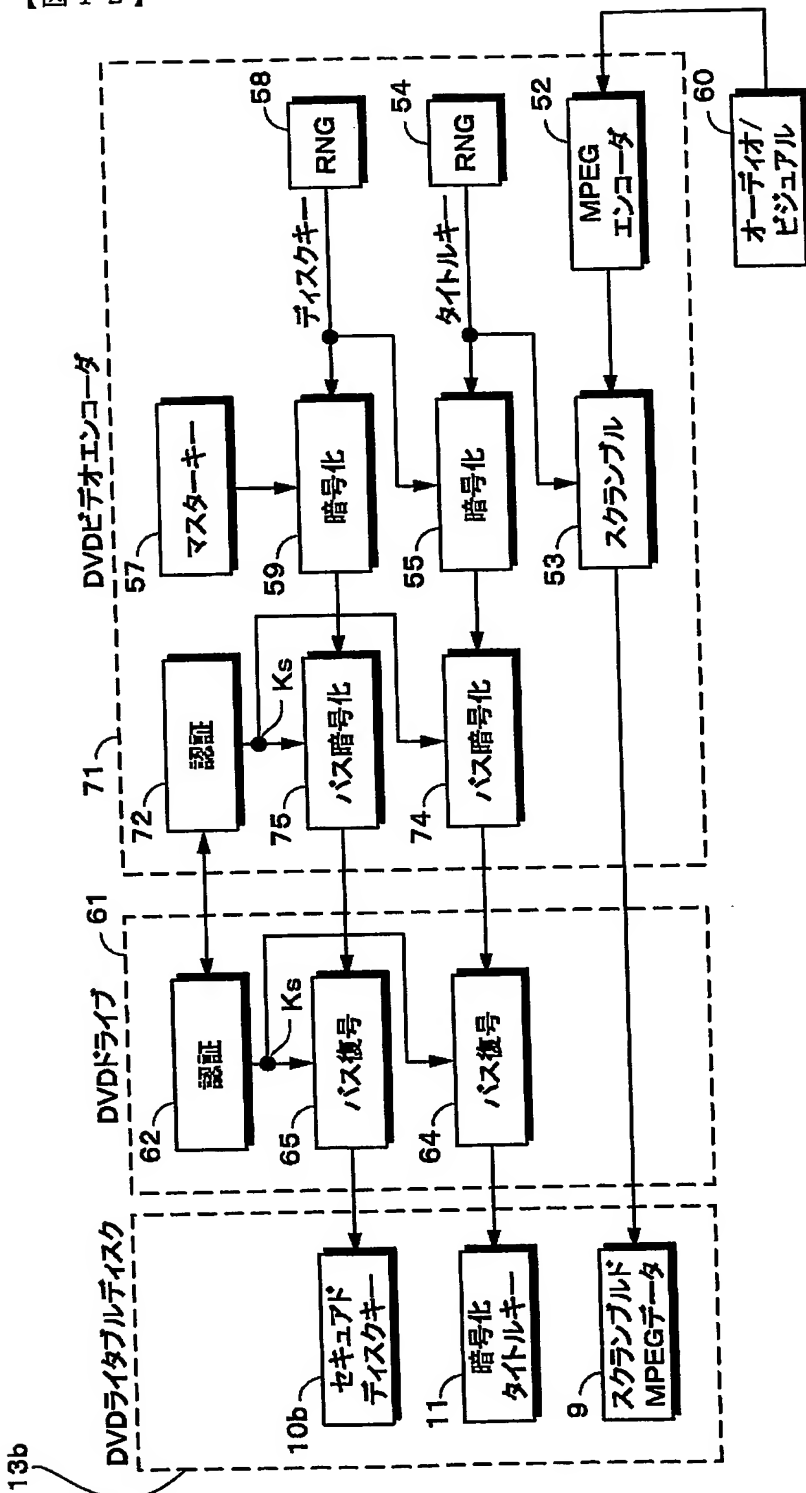
【図10】



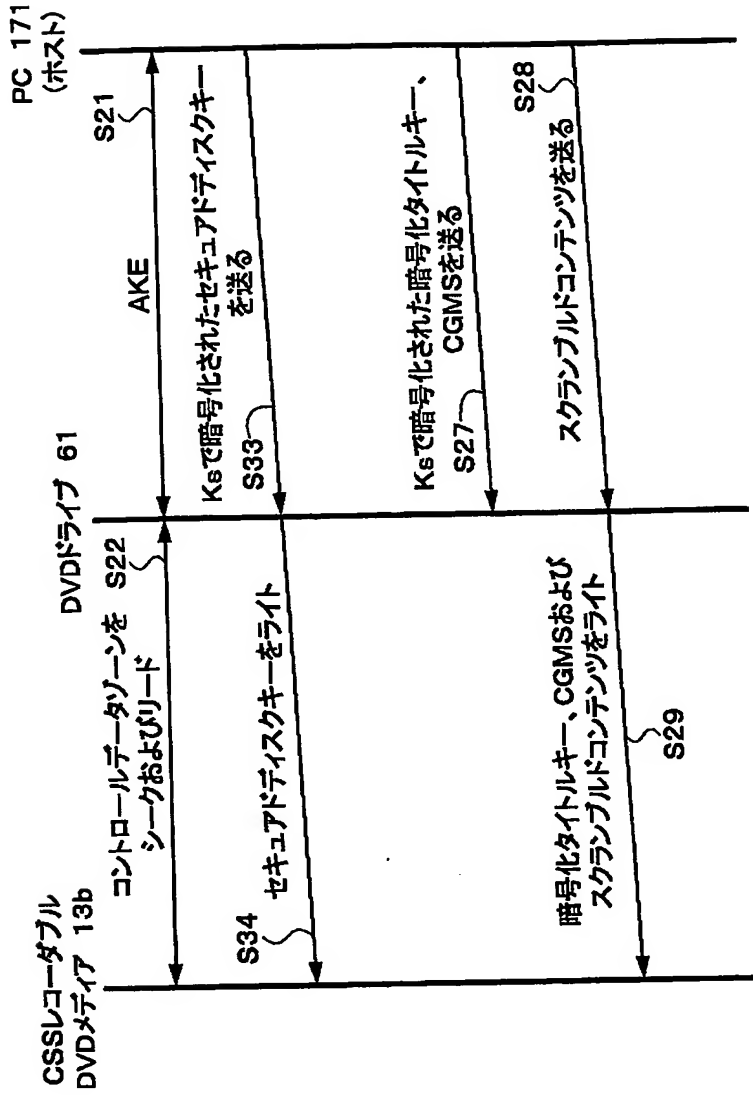
【図 11】



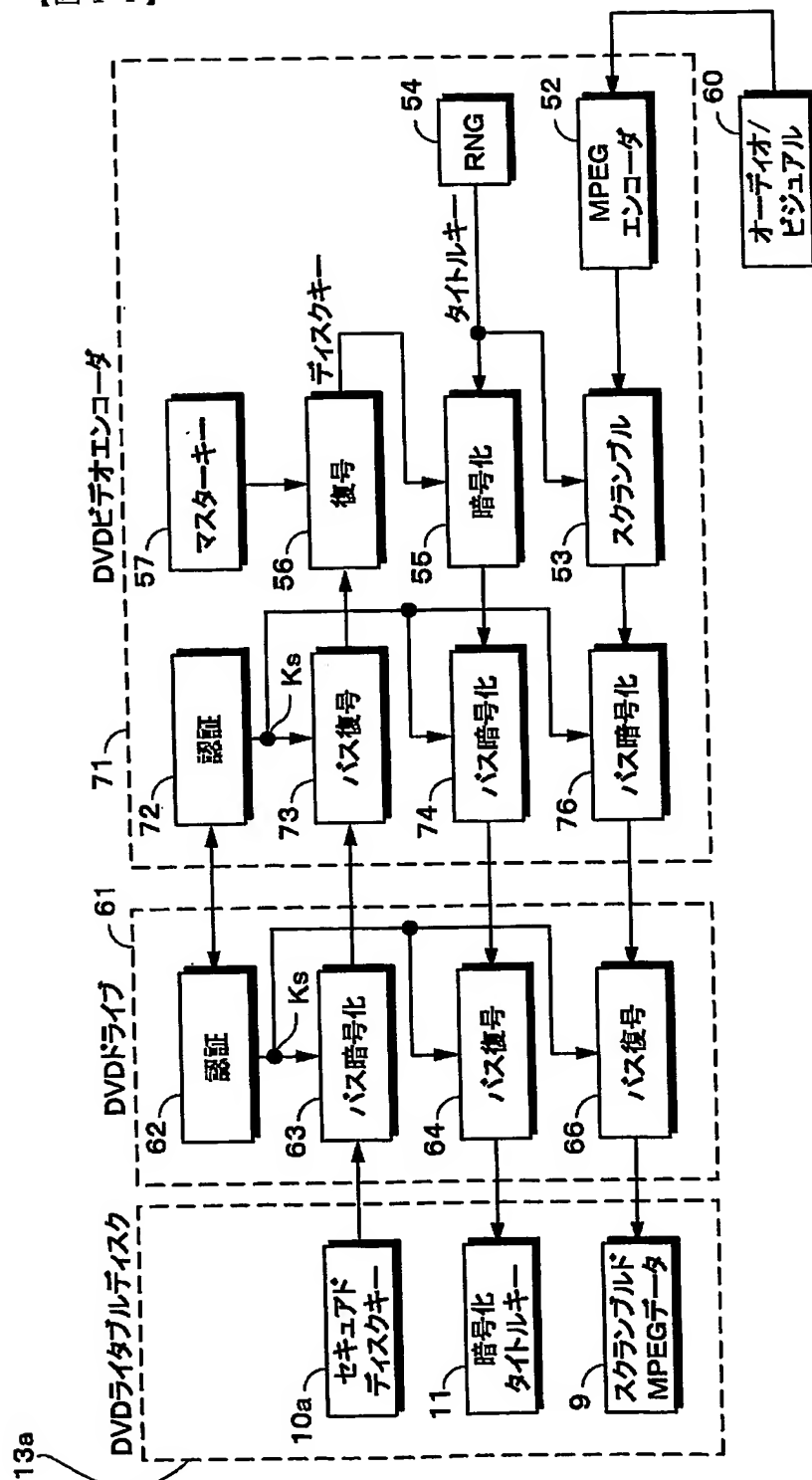
【図 12】



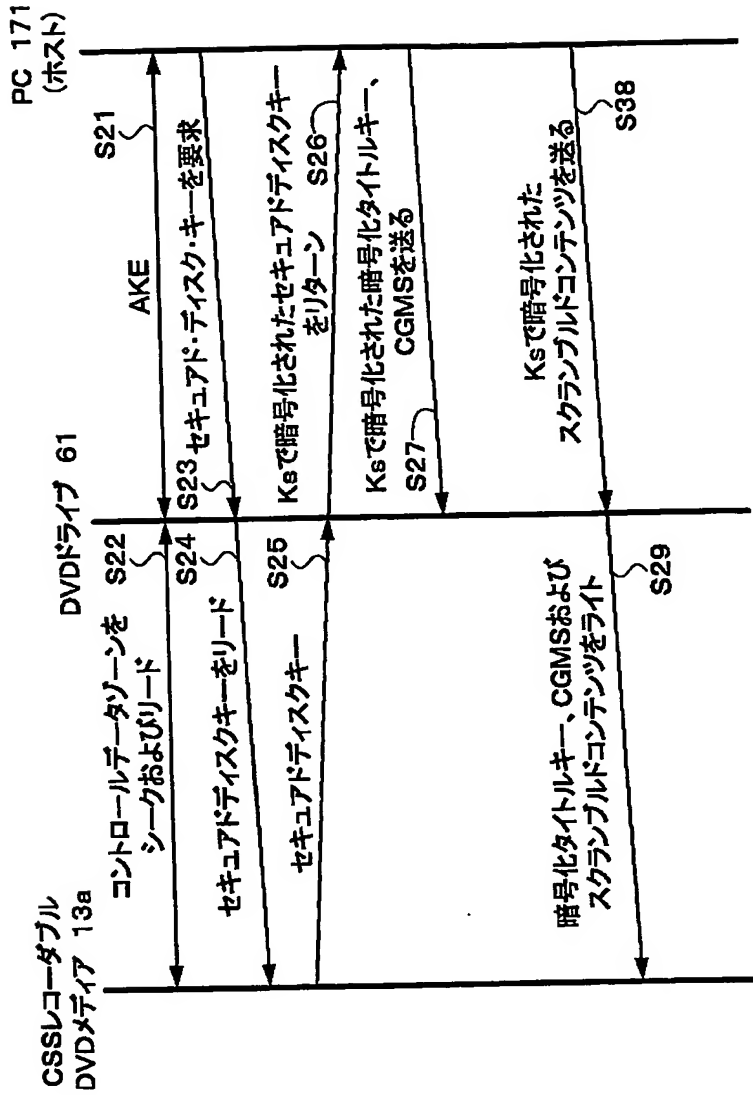
【図 13】



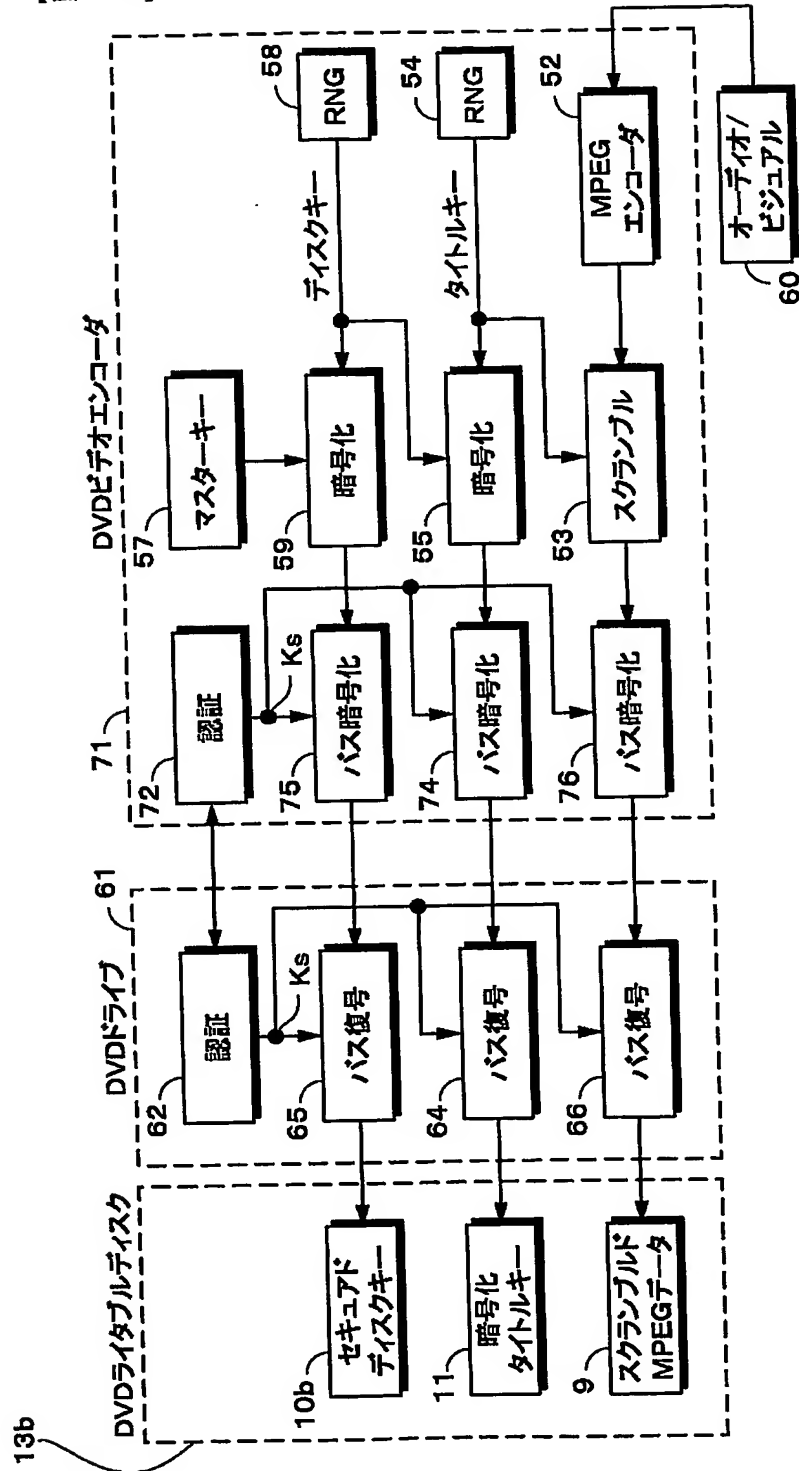
【図 14】

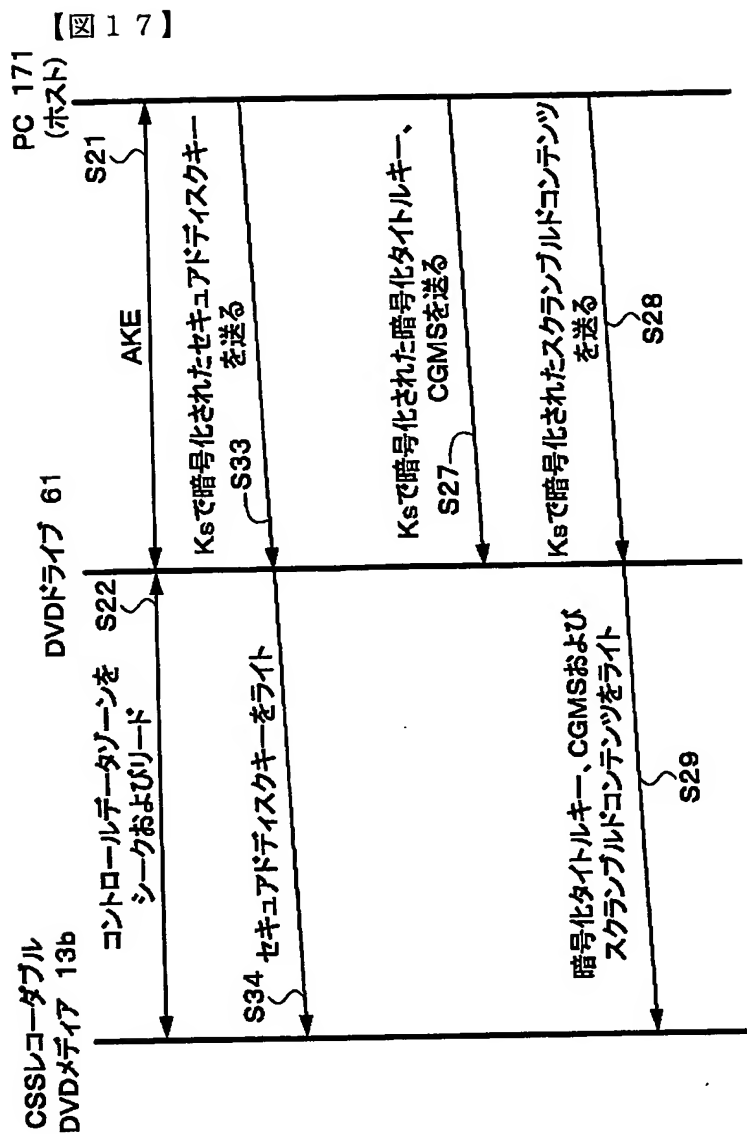


【図 15】

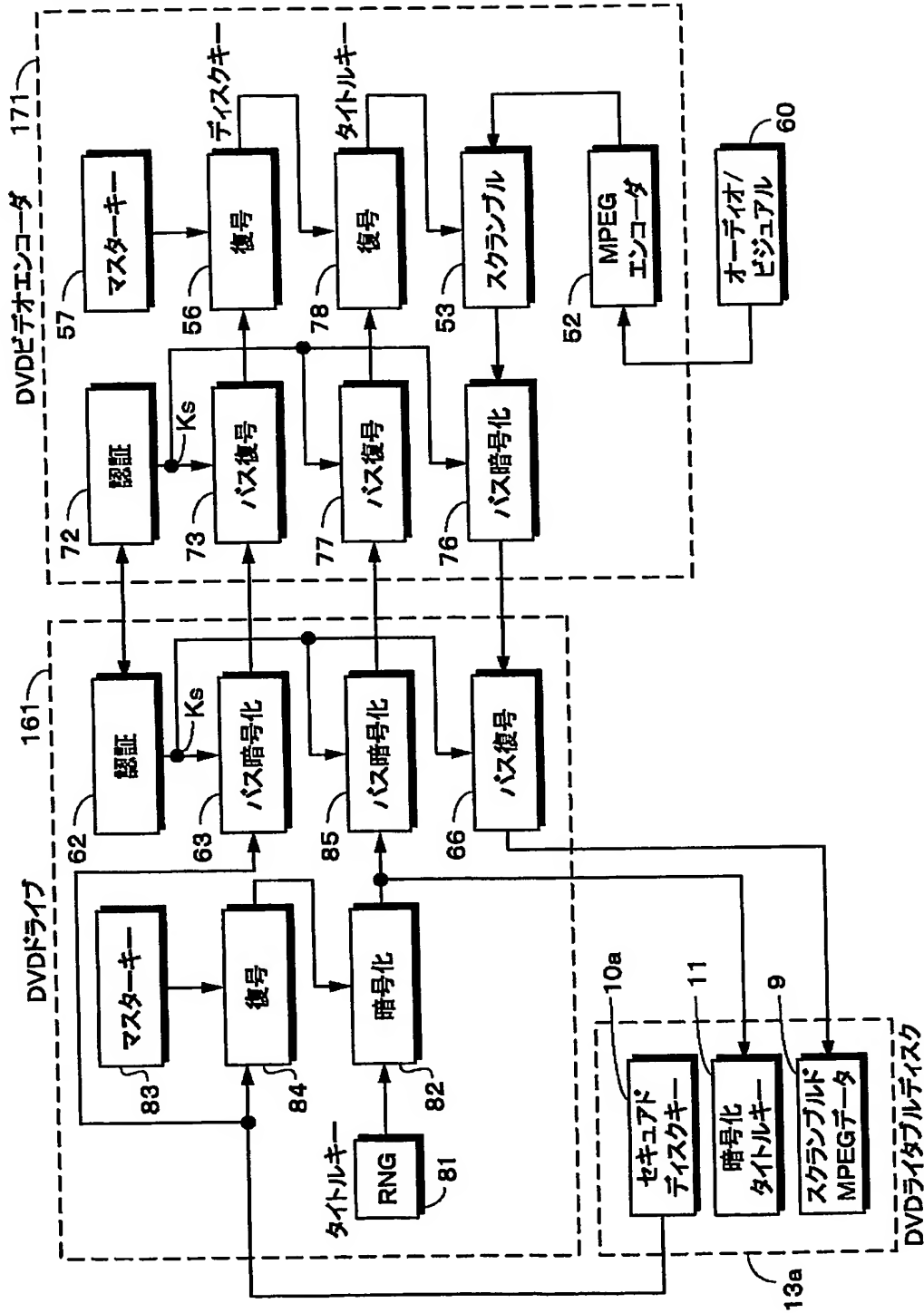


【図 16】

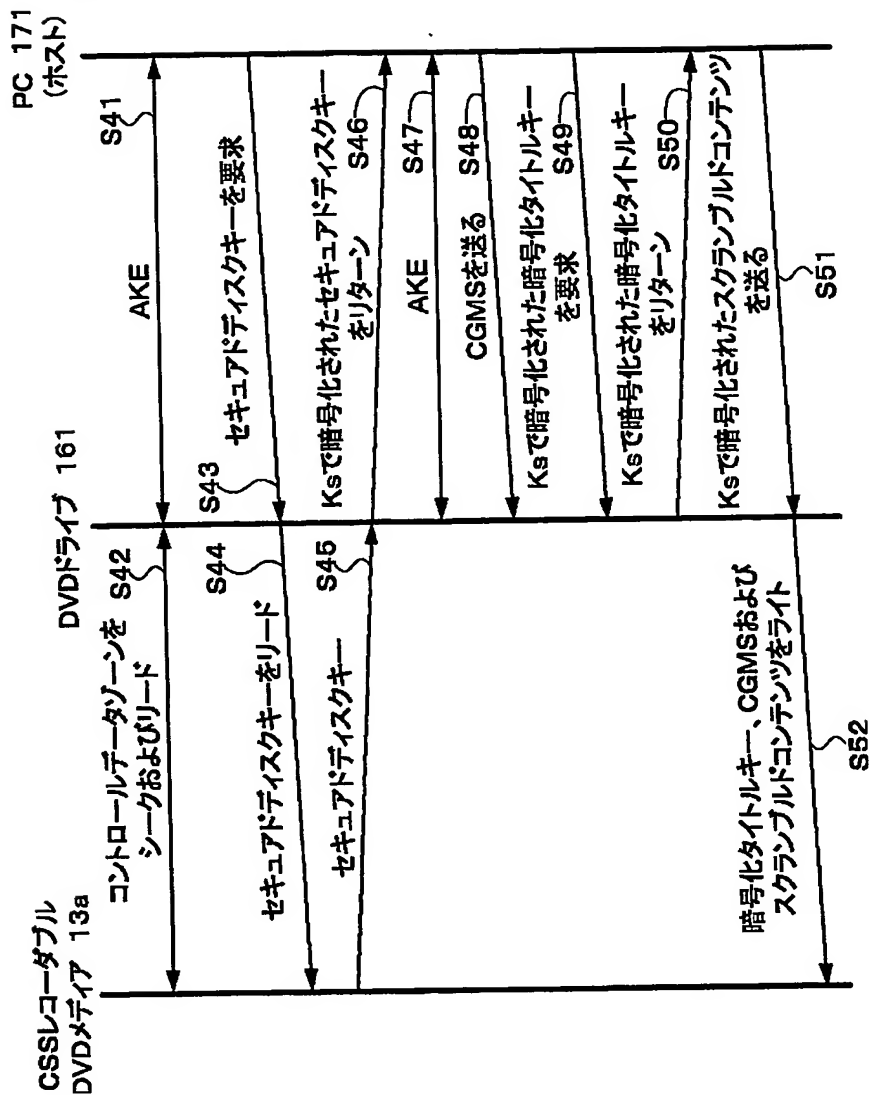




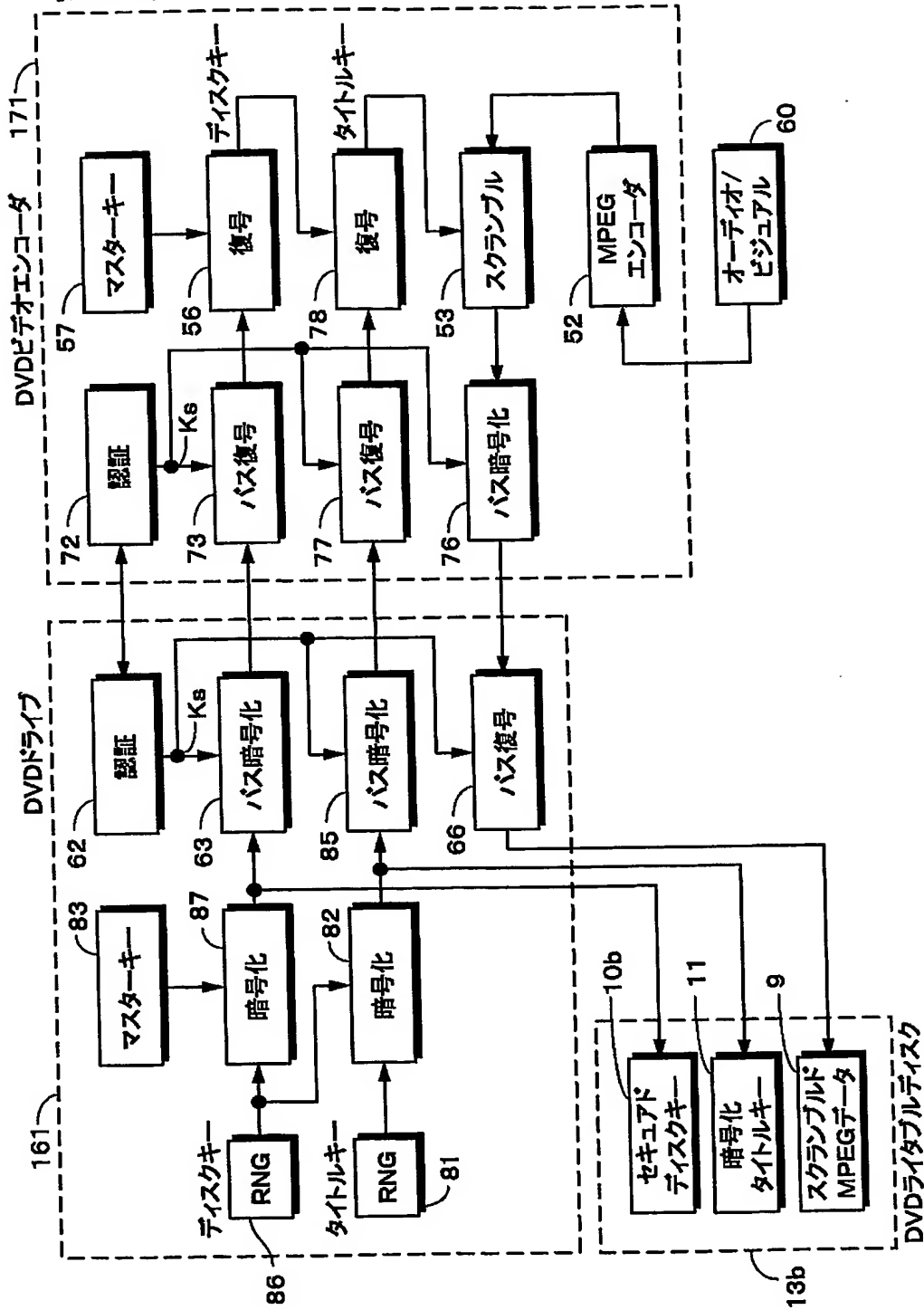
【図 18】



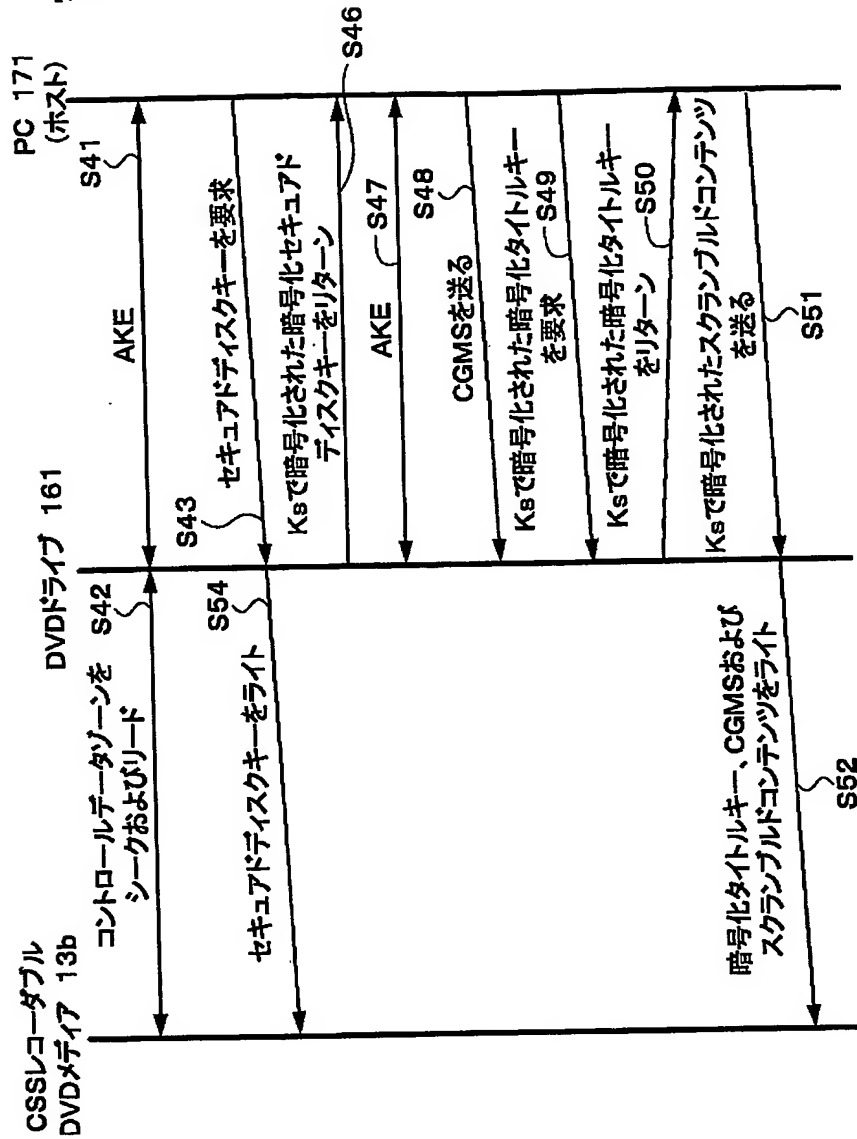
【図 19】



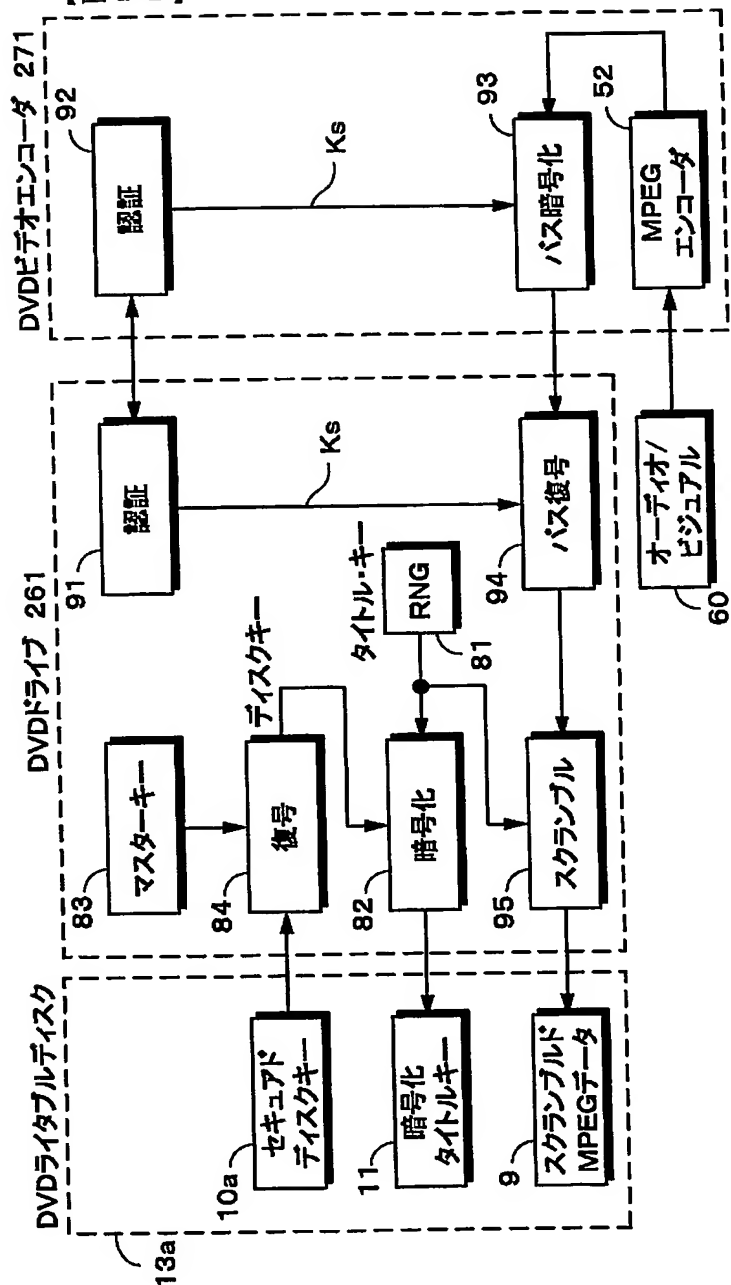
【図 20】



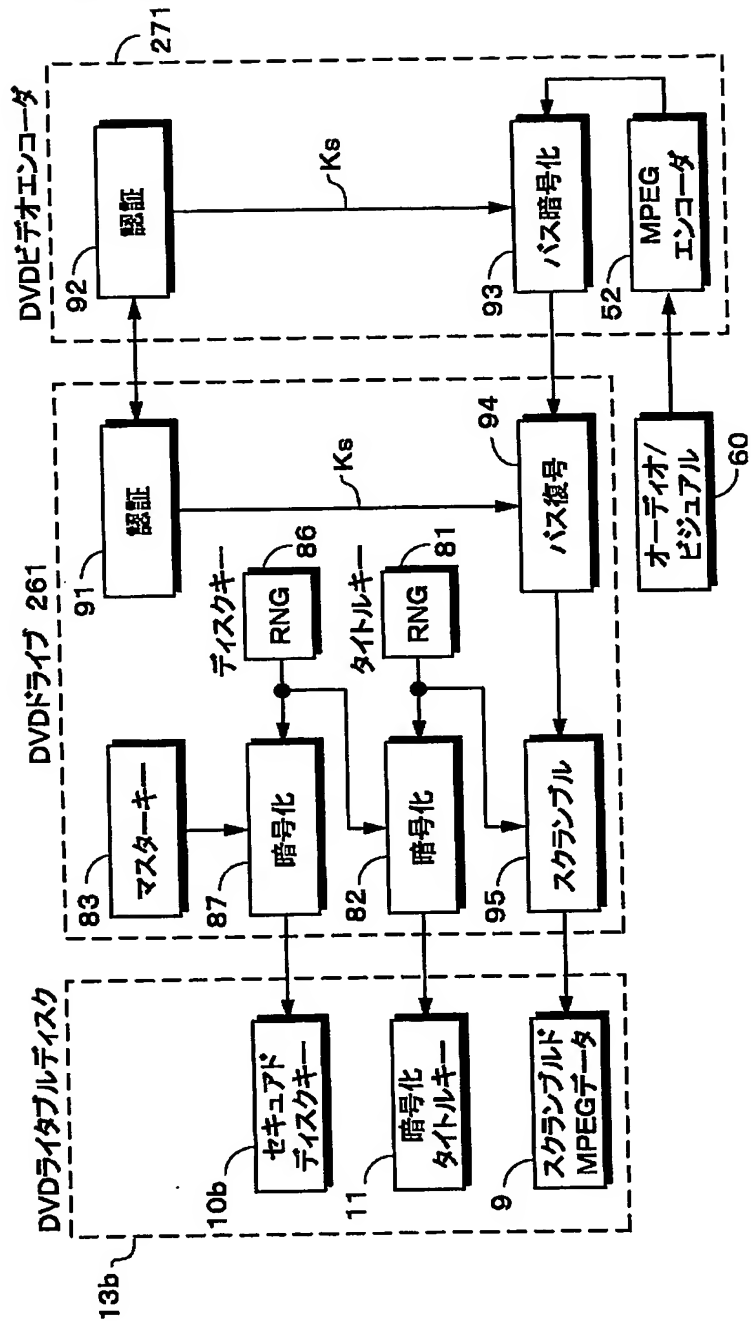
【図 21】



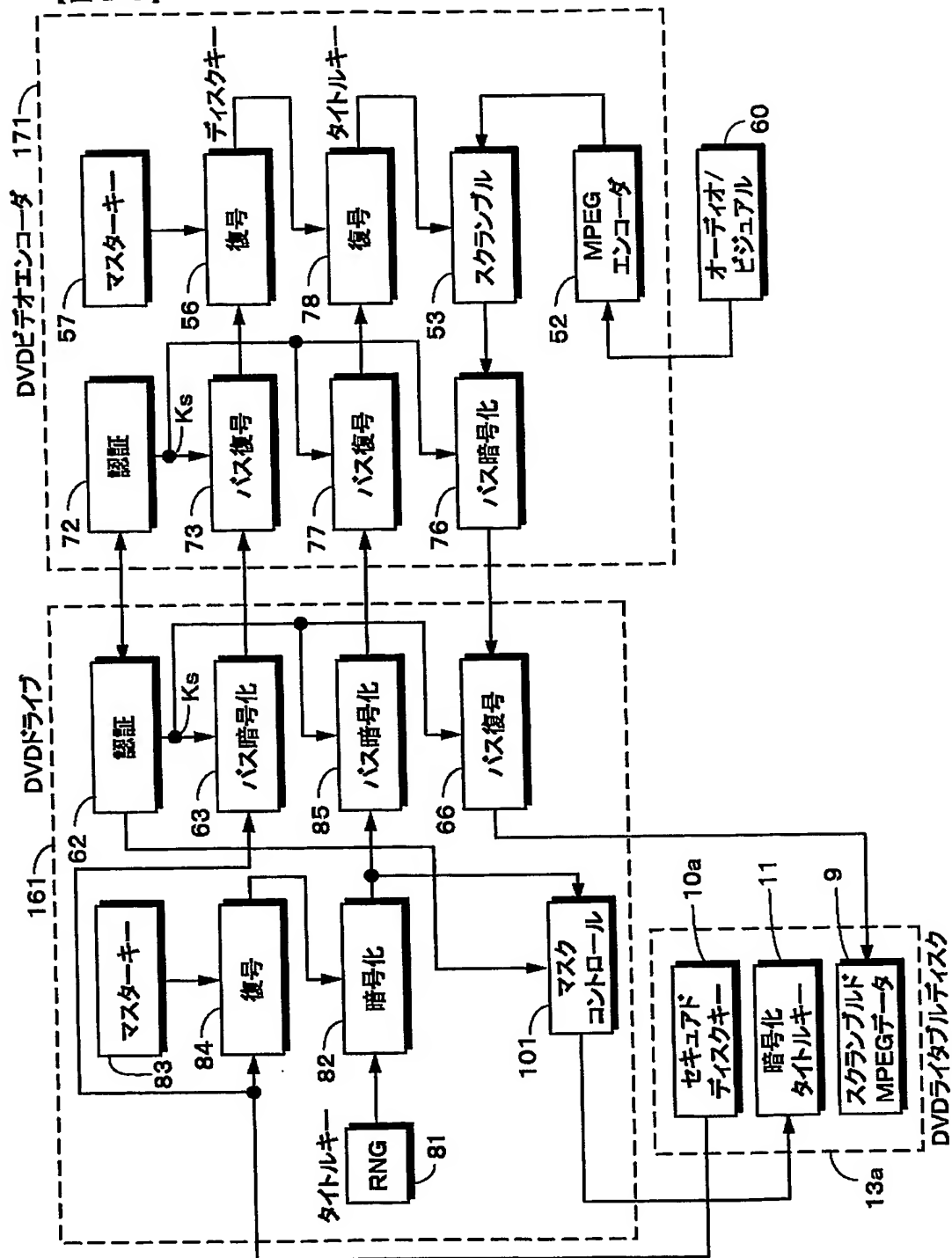
【図 22】



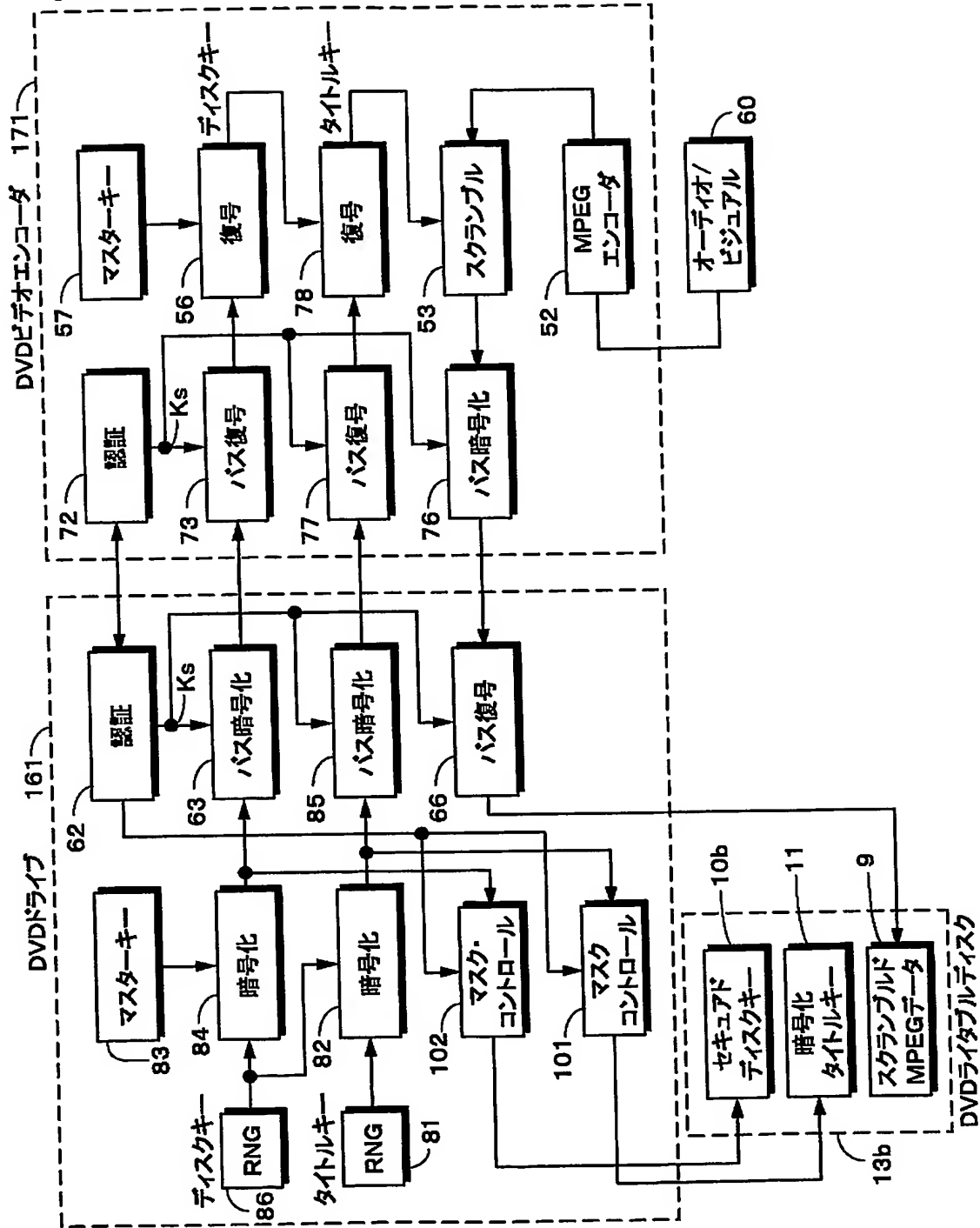
【図 23】



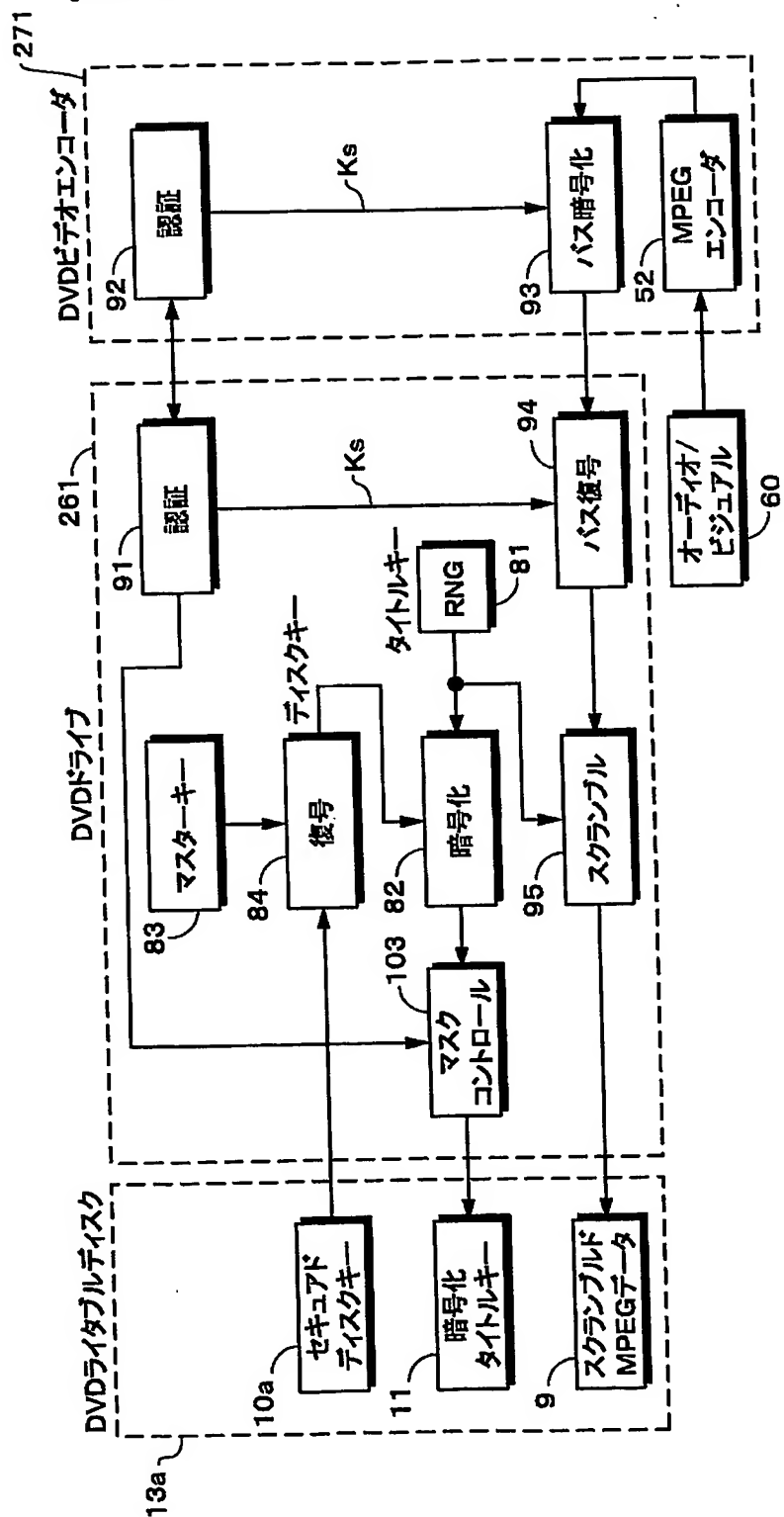
【圖 24】



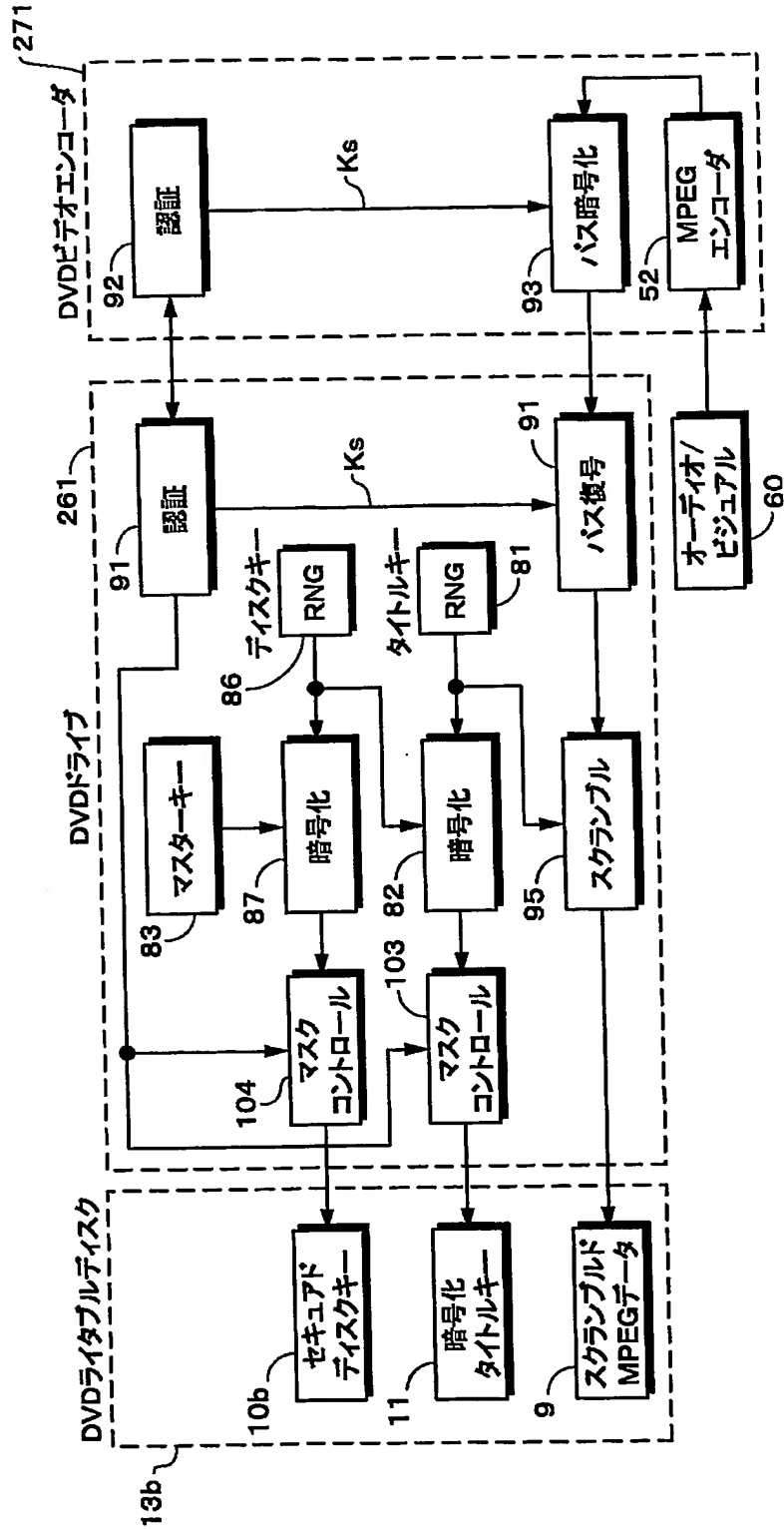
【図 25】



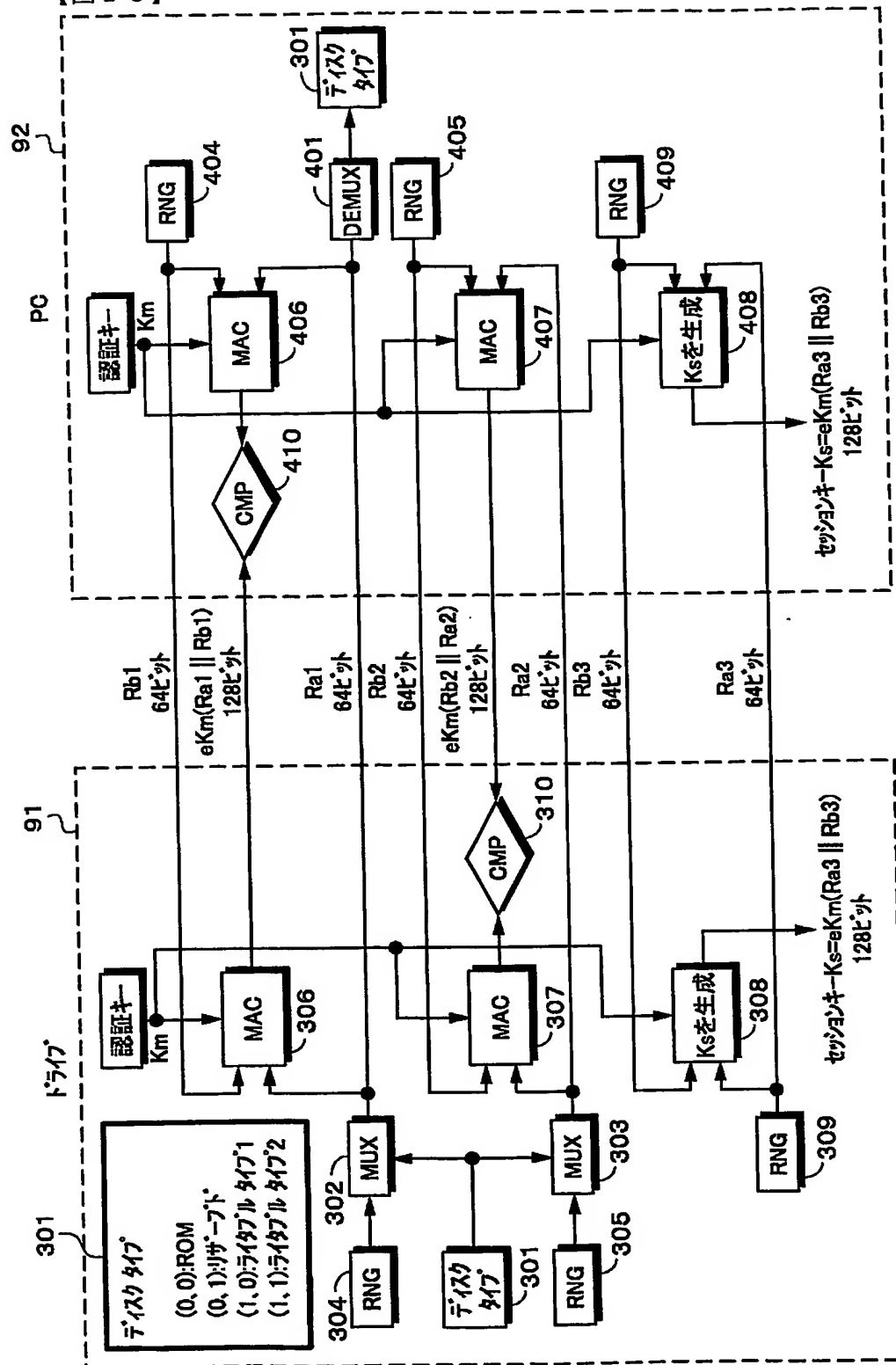
【図 26】



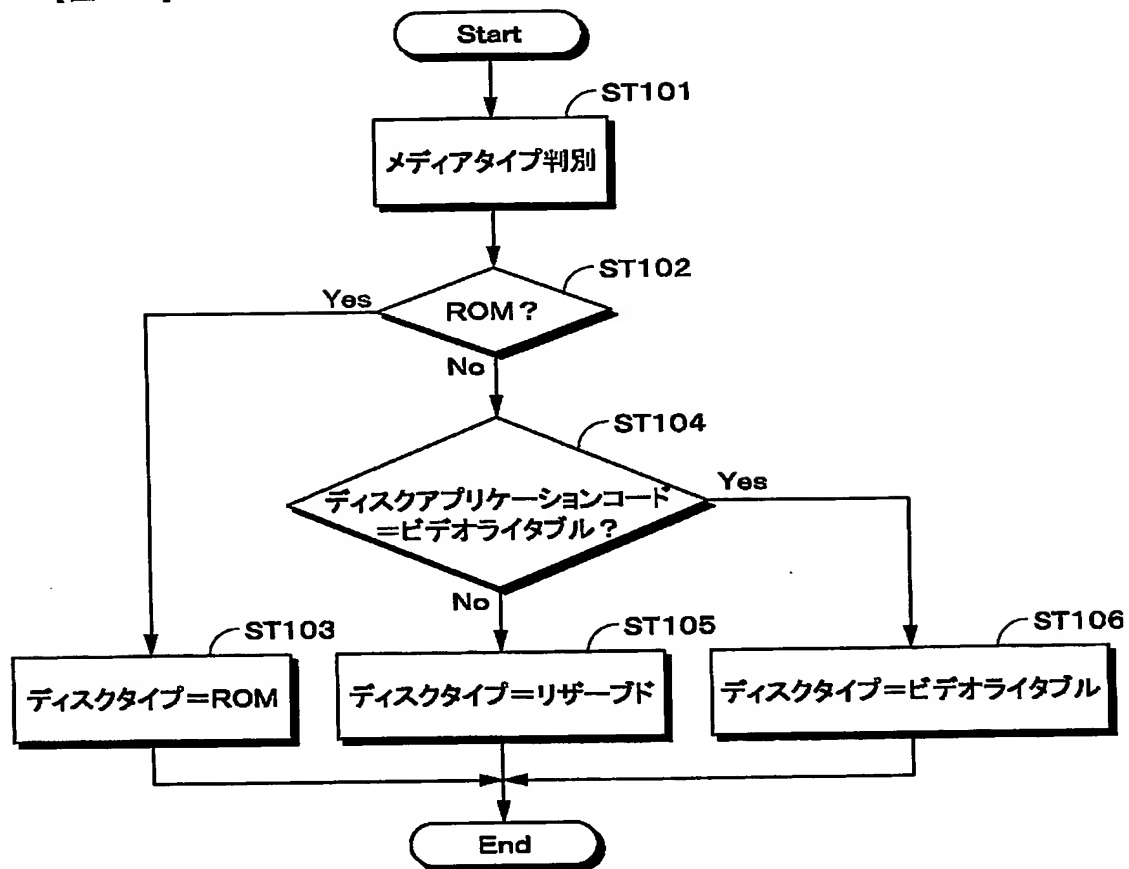
【図 27】



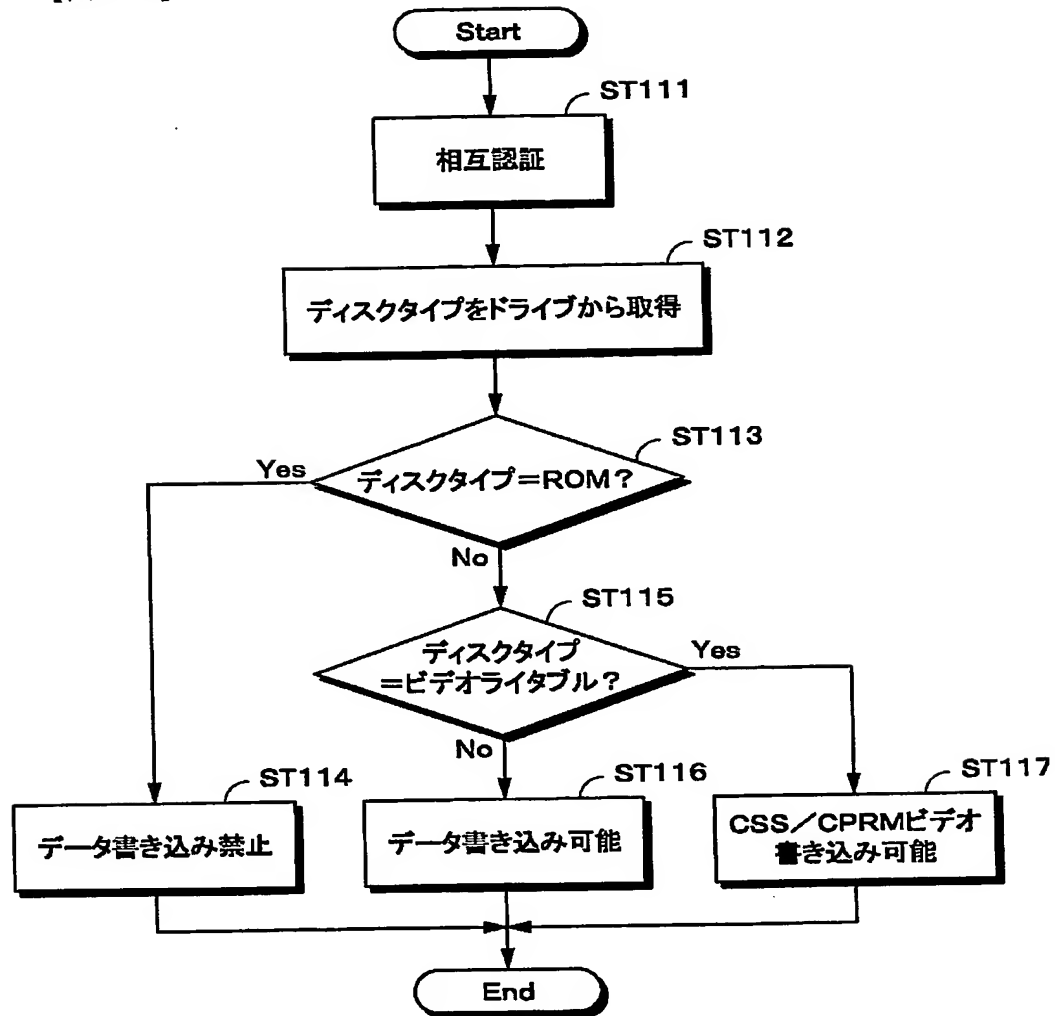
【図 28】

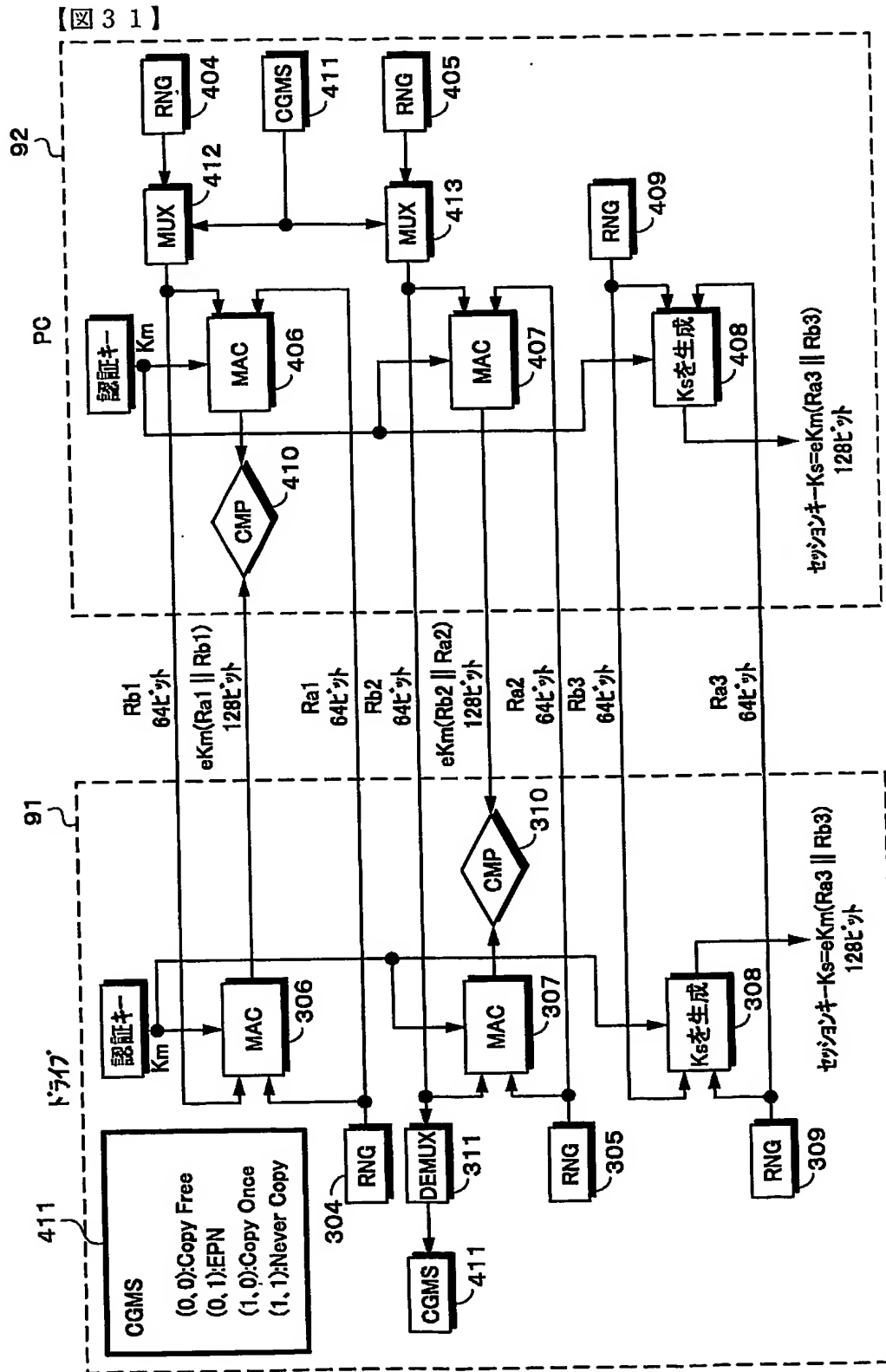


【図 29】

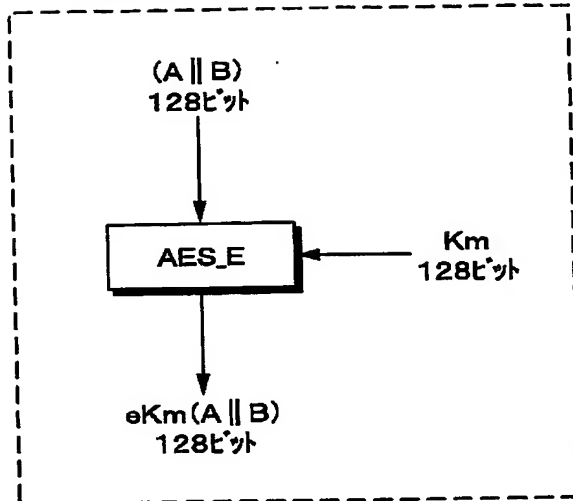


【図30】



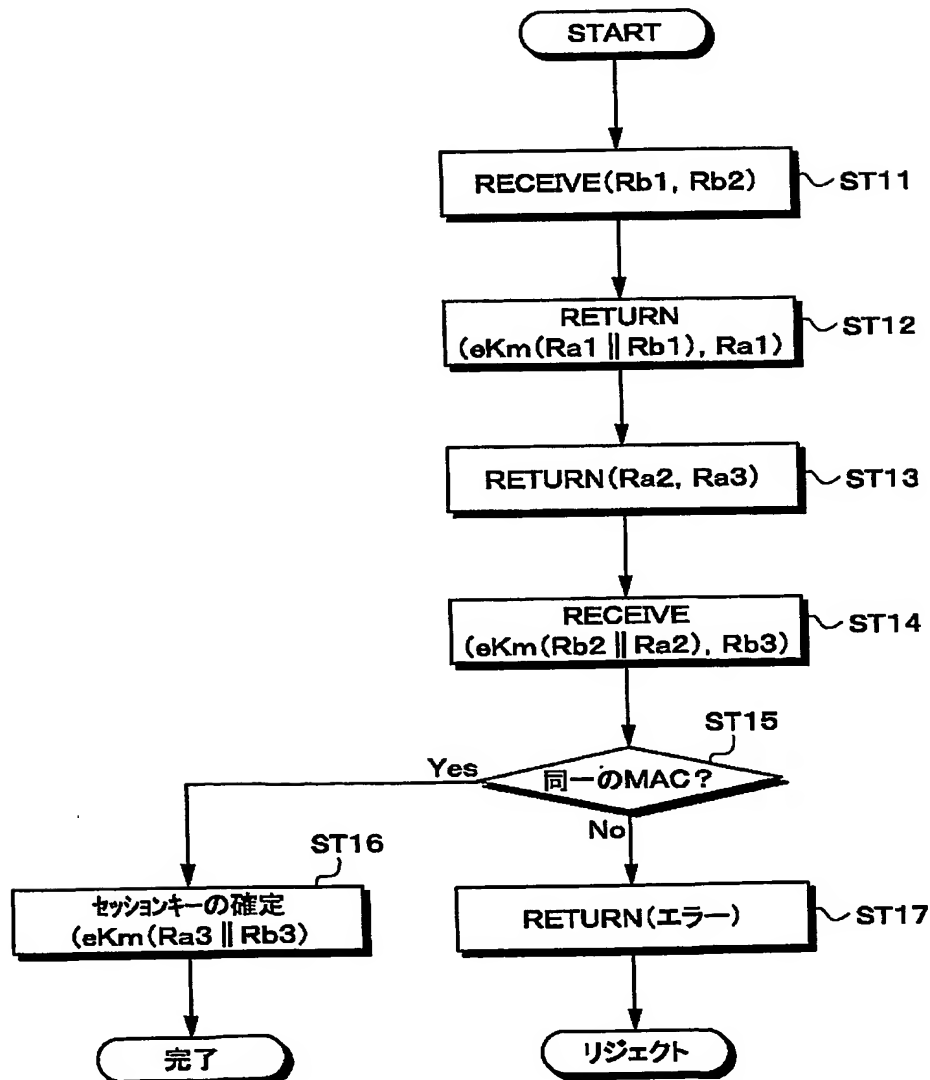


【図 3 2】

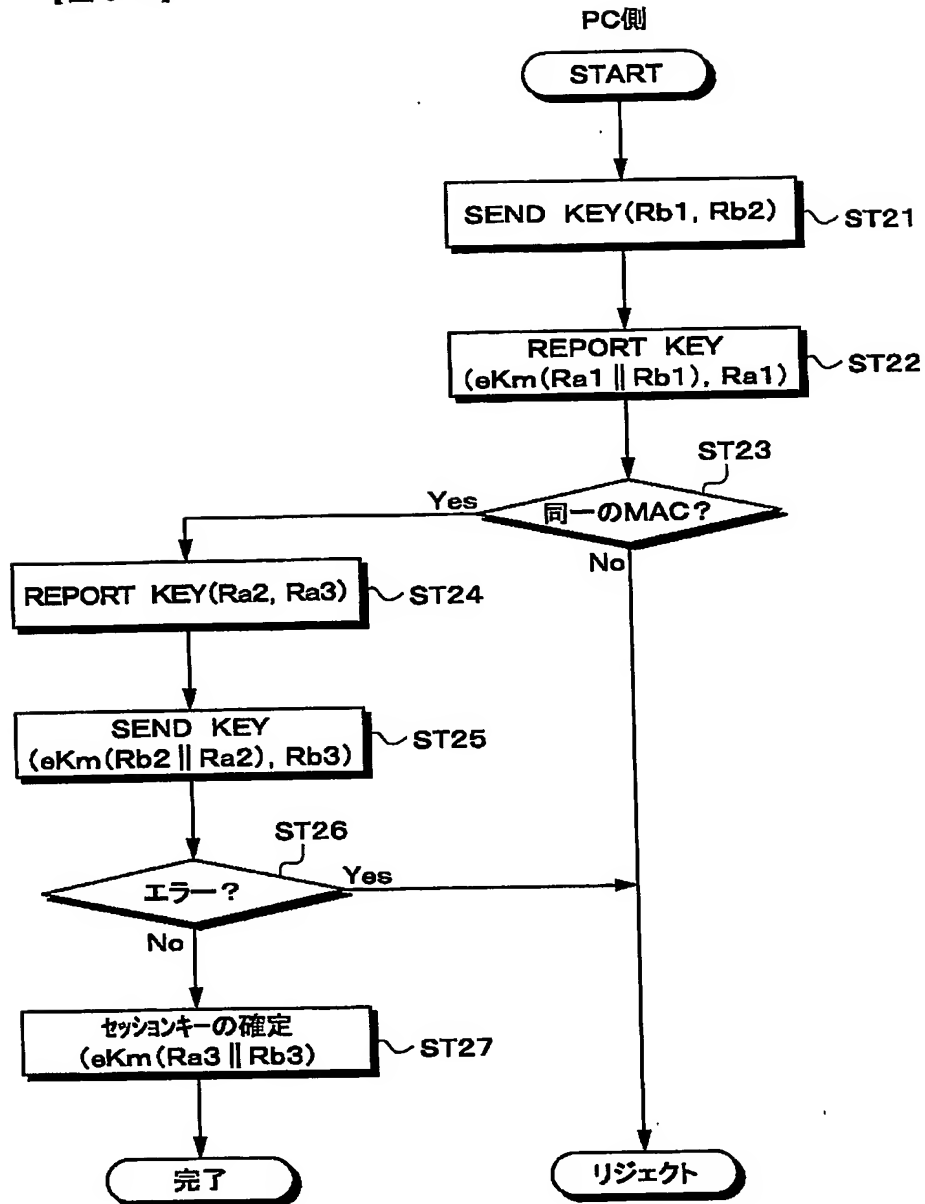


【図 3 3】

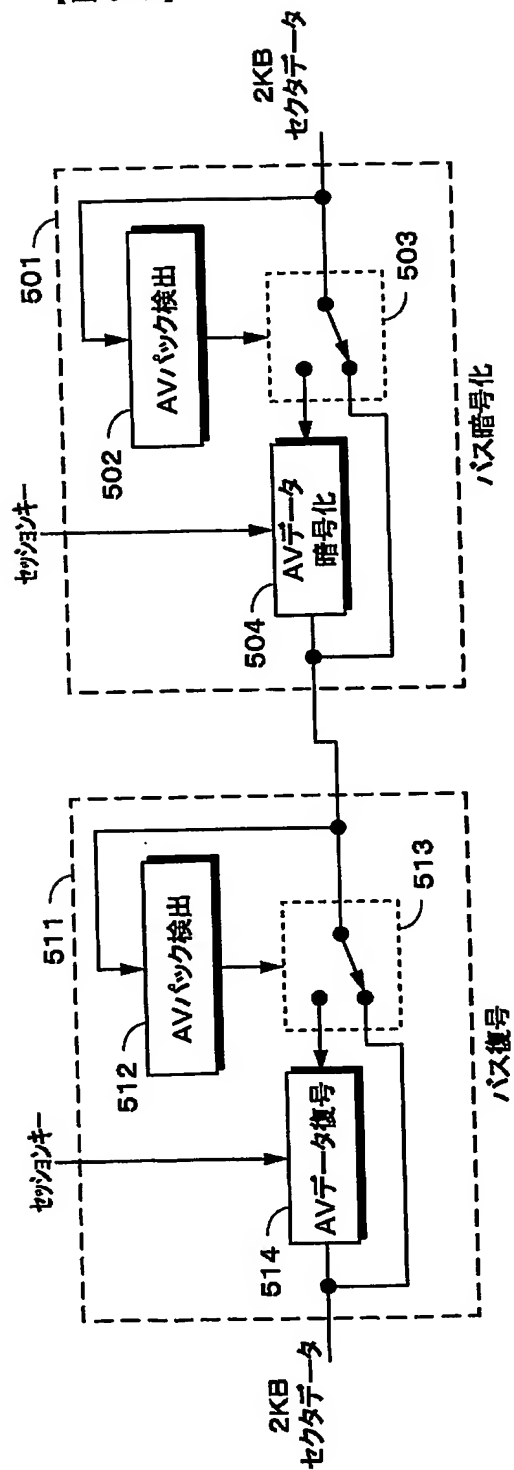
DVDドライブ側



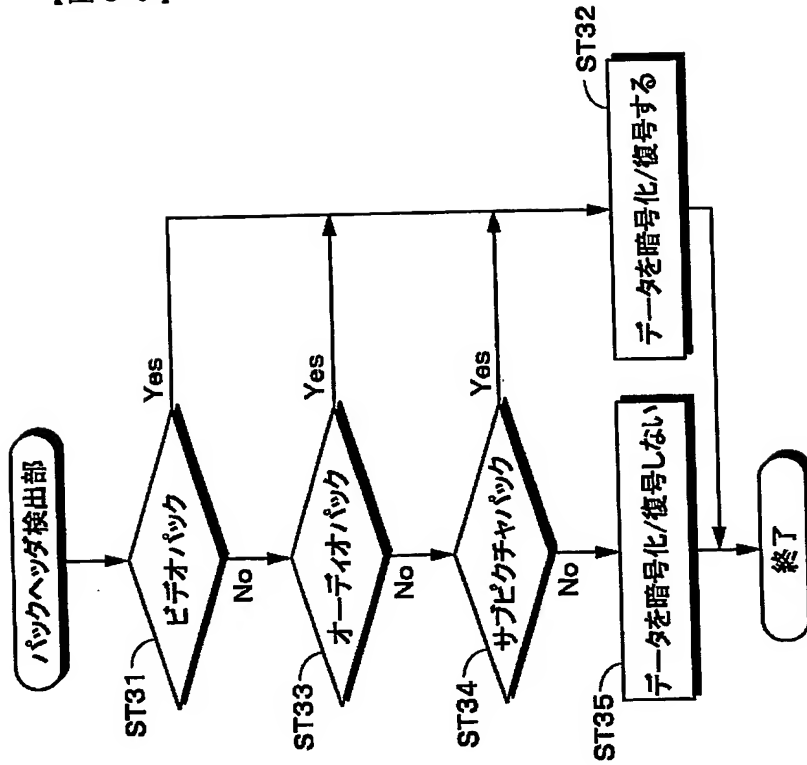
【図 34】



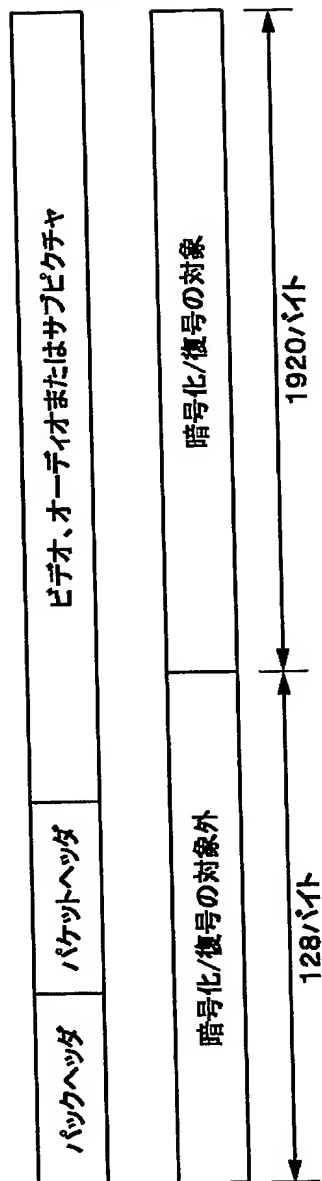
【図 35】



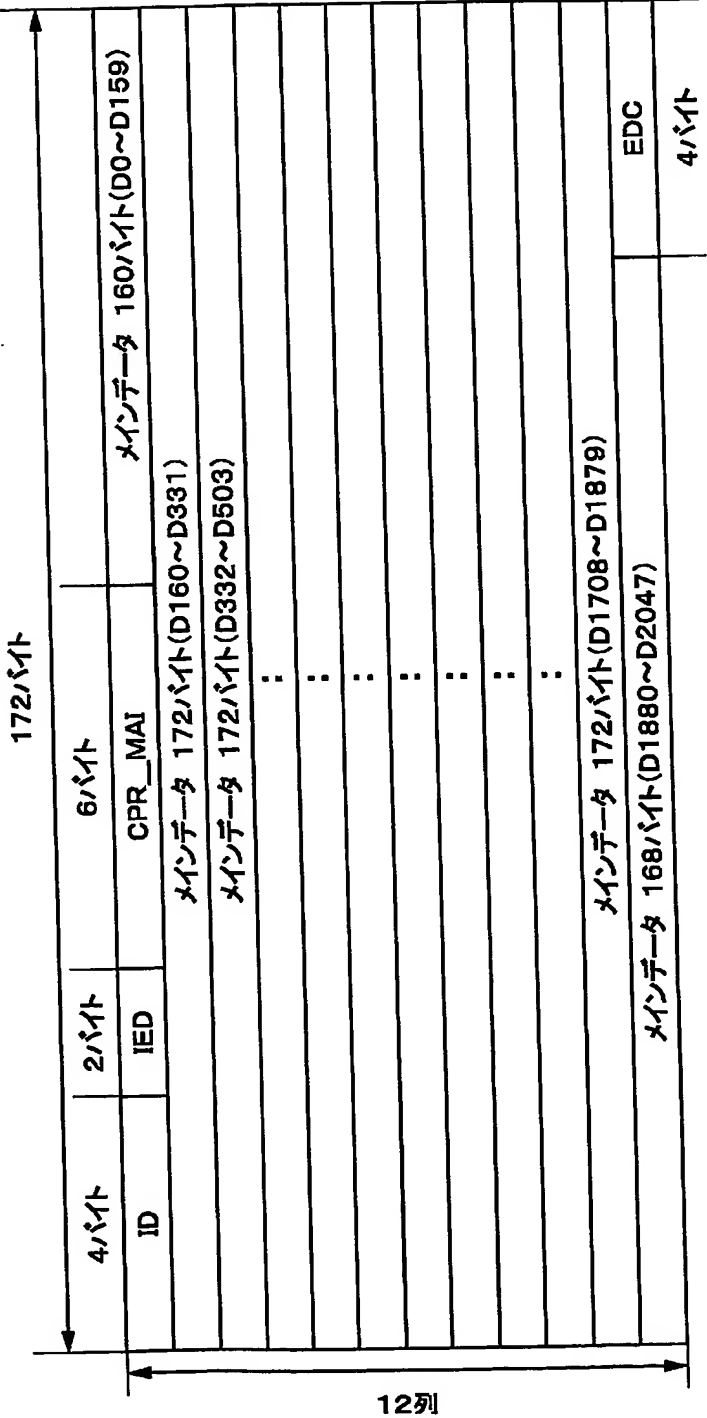
【図 36】



【図 37】

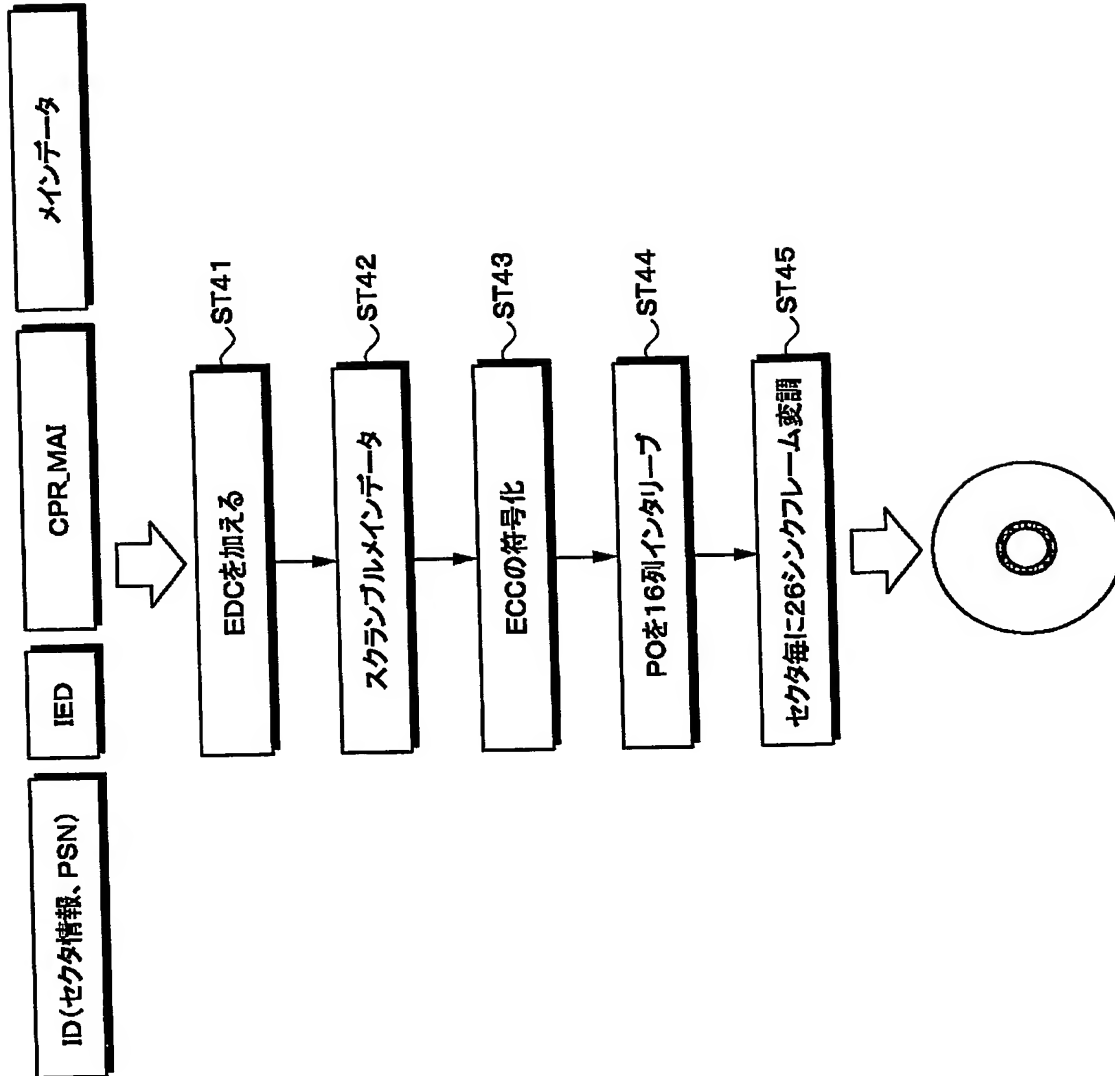


【図 38】



セクタ構成例

【図 39】



【図 40】

B

CPM	CP- SEC	CGMS	CPS_MOD
BP0	暗号化されたビデオタイトルキー(MSB)		
BP1	暗号化されたビデオタイトルキー		
BP2	暗号化されたビデオタイトルキー		
BP3	暗号化されたビデオタイトルキー		
BP4	暗号化されたビデオタイトルキー		
BP5	暗号化されたビデオタイトルキー(LSB)		

データエリア内におけるCPR_MAI(CSS)

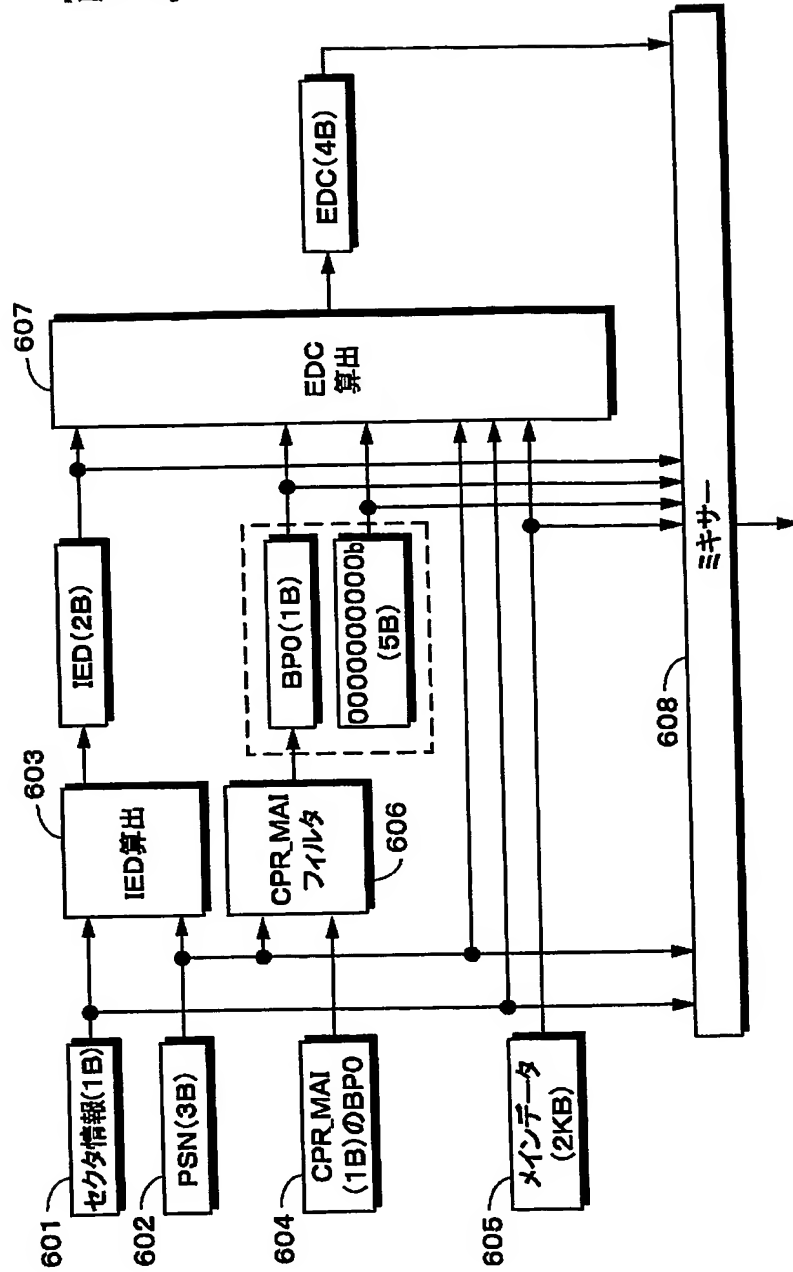
A

著作権保護システムタイプ
セキュアディスクキーデータモード
リザーブド
リザーブド
リザーブド
ビデオ認証コントロールコード
地域管理情報

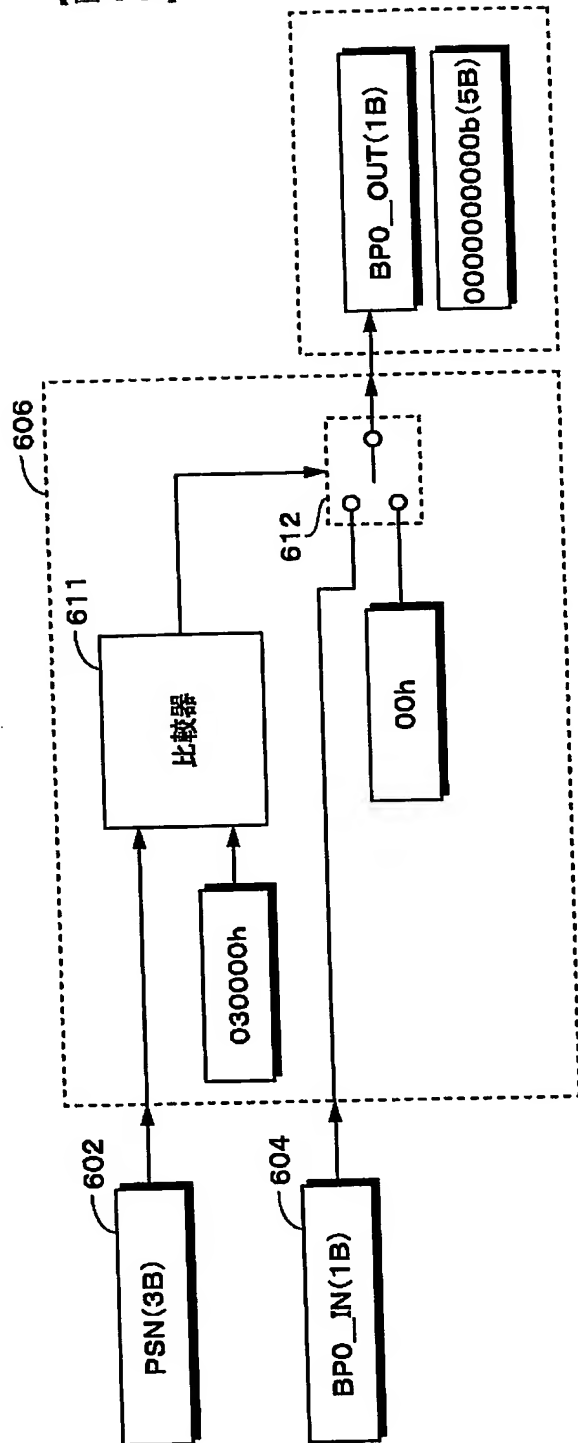
リードインエリア内におけるCPR_MAI

... マスキングエリア

【図41】

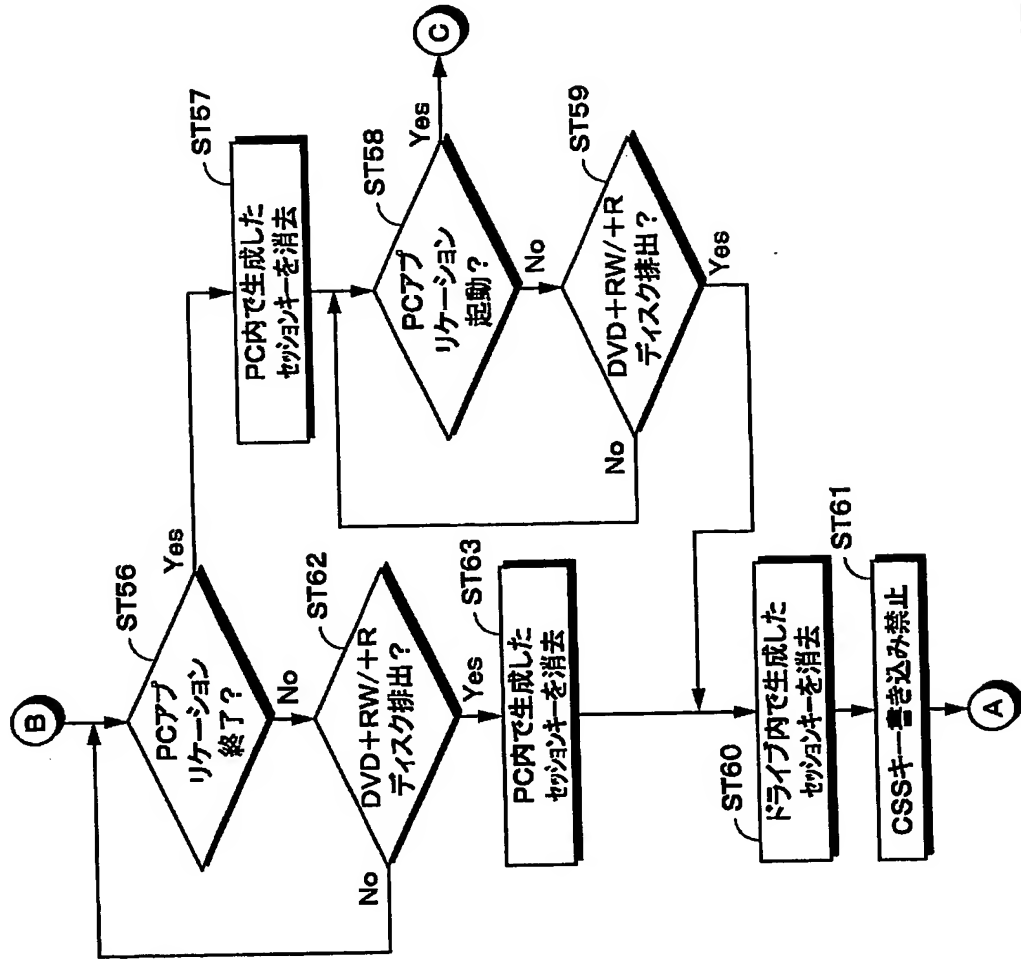


【図 42】

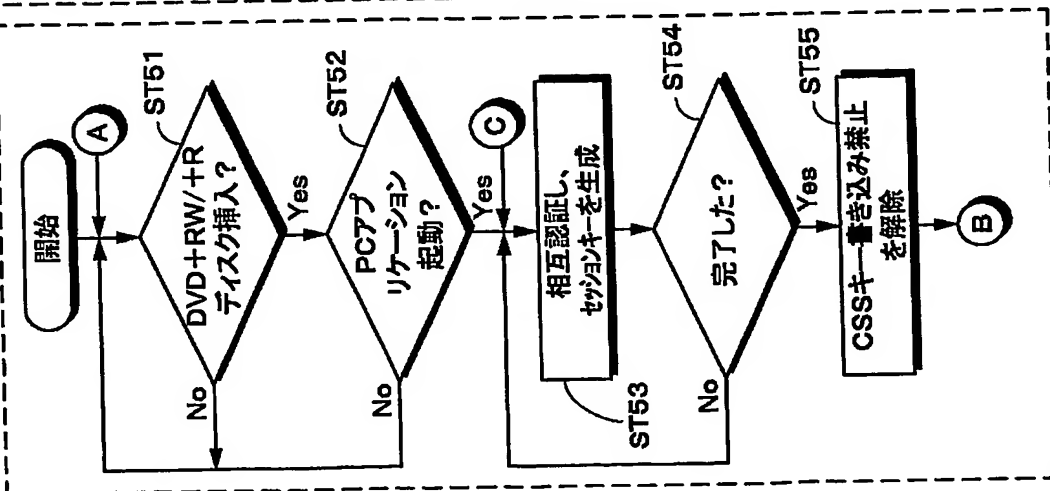


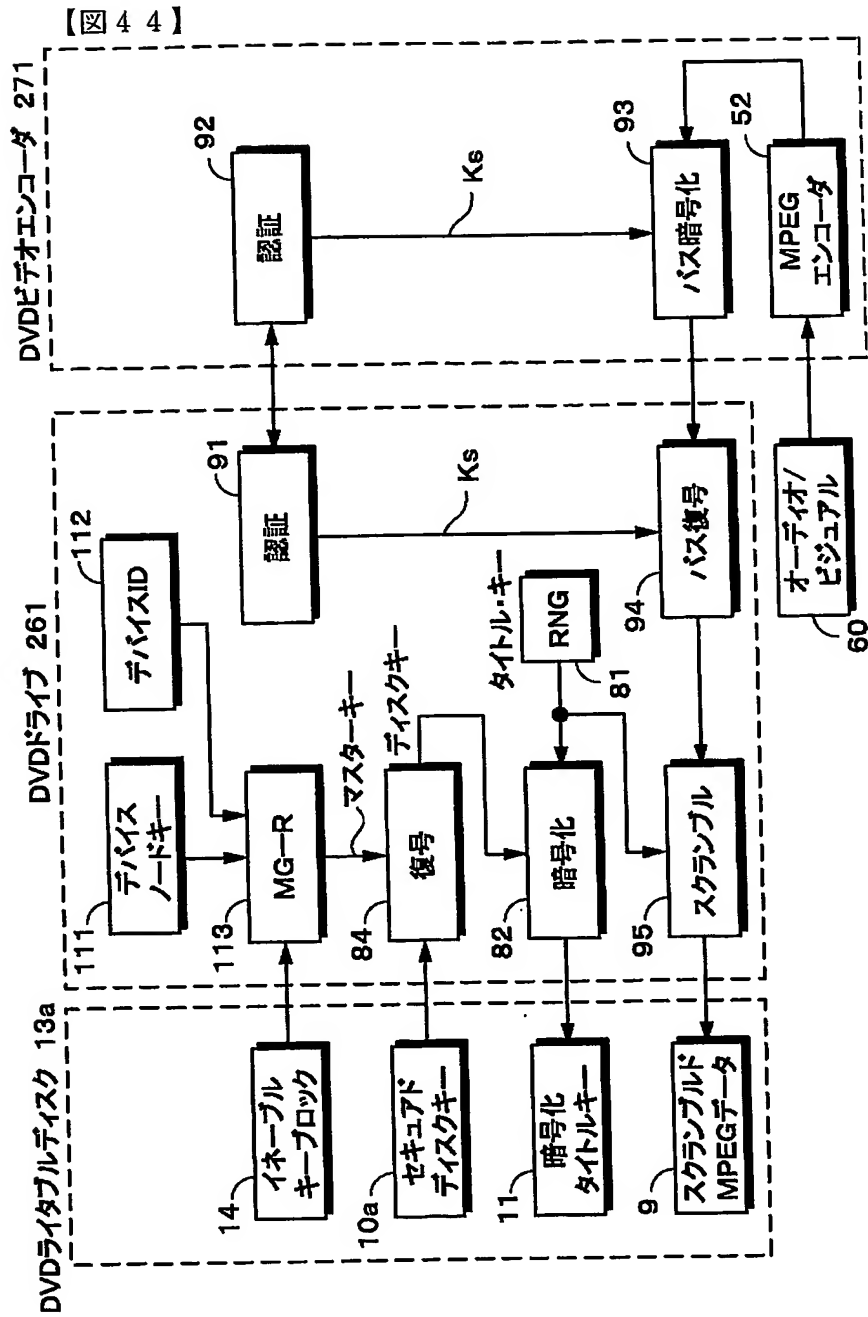
【図 4 3】

セッションキーの消滅



セッションキーの生成





【書類名】 要約書

【要約】

【課題】 著作権保護技術で書き込みデータを保護し、一般ユーザによる著作権保護技術の書き込みソフトウェアを作成させない。

【解決手段】 予めセキュアドディスクキー 10 a が記録されているライタブルディスク 13 a が使用される。ドライブ 161 は、タイトルキーを生成する乱数発生器 81 と、生成したタイトルキーをディスクキーで暗号化するエンクリプタ 82 と、マスターキー 83 と、セキュアドディスクキーをマスターキーで復号するデクリプタ 84 とを内部に備えている。さらに、セッションキー Ks を生成する認証部 62、セッションキー Ks でセキュアドディスクキーを暗号化するバスエンクリプタ 63、スクランブルド MPEG データを復号するバスデクリプタ 66 が備えられている。暗号化のための鍵がドライブ内にあるために、一般ユーザが CSS 書き込みソフトウェアを勝手に作成できない。

【選択図】 図 18

特願 2 0 0 3 - 3 4 0 0 7 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社